RESUMEN – TRABAJO DE GRADO

AUTORES	AURA LUCIA CASADIEGOS SANTANA MARCELA QUINTERO JIMÉNEZ MILEIDY TORO RUEDA
FACULTAD	FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS	ESPECIALIZACION EN AUDITORIA DE SISTEMAS
DIRECTOR	TORCOROMA VELÁSQUEZ PÉREZ
TÍTULO DE LA TESIS	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL ÁREA DE CONTABILIDAD DE LA E.S.E. HOSPITAL LOCAL DE RIO DE ORO CESAR

RESUMEN

(70 palabras aproximadamente)

Mediante un SGSI – Sistema de Gestión de Seguridad de la Información, el Área de Contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar conseguirá minimizar considerablemente el riesgo de que su productividad se vea afectada debido a la ocurrencia de un evento que comprometa la confidencialidad, disponibilidad e integridad de la información o de alguno de los sistemas informáticos. Este sistema permite identificar, gestionar y minimizar los riesgos reales y potenciales de la seguridad de la información, de una forma documentada, sistemática, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías

CARACTERÍSTICAS

PÁGINAS: 153	PLANOS:	ILUSTRACIONES:	CD-ROM: 1

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL ÁREA DE CONTABILIDAD DE LA E.S.E. HOSPITAL LOCAL DE RIO DE ORO CESAR

AURA LUCIA CASADIEGOS SANTANA
MARCELA QUINTERO JIMÉNEZ
MILEIDY TORO RUEDA

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
ESPECIALIZACION EN AUDITORIA DE SISTEMAS
OCAÑA
2014

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL ÁREA DE CONTABILIDAD DE LA E.S.E. HOSPITAL LOCAL DE RIO DE ORO CESAR

AURA LUCIA CASADIEGOS SANTANA
MARCELA QUINTERO JIMÉNEZ
MILEIDY TORO RUEDA

Trabajo de Grado presentado para optar el título de Especialista en Auditoria de Sistemas

Director
TORCOROMA VELÁSQUEZ PÉREZ
I.S. E.S.P. MSC. Ciencias Computacionales

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
ESPECIALIZACION EN AUDITORIA DE SISTEMAS
OCAÑA
2014

CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

INTRODUCCIÓN

Actualmente nos encontramos en una época en la que la información y los datos poseen una importancia decisiva en la gran mayoría de empresas, convirtiéndose así en uno de sus activos más importantes. De igual forma, la tecnología actualmente permite la circulación ilimitada de información a través de las redes locales y de Internet, además permite compartir datos y realizar operaciones en forma remota, potenciando la productividad de las personas, si bien es cierto esto es muy importante para las empresas ya que les permite un mayor desarrollo, por contrapartida se tiene la aparición de nuevos riesgos, que van a afectar directamente a aquello que le da valor a toda compañía: su información. Los delitos informáticos se han vuelto la opción de un creciente grupo de delincuentes discretos que hacen uso de la tecnología emergente de manera inapropiada.

Es por esta razón que las empresas han comenzado a tomar conciencia y a proteger aquellos recursos de información que son cruciales para ellos, buscando así brindar una protección adecuada sobre estos. Para ello, las distintas empresas buscan asegurar la integridad, confidencialidad y disponibilidad de la información.

Con el presente proyecto se pretende incorporar un sistema de gestión de seguridad de información para el Área de contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar, que le permitirá poder identificar los riesgos que atenten contra los recursos de la misma y tratar de mitigarlos, implementando ciertos controles capaces de brindar un nivel aceptable de seguridad.

El documento está compuesto por los siguientes capítulos:

CAPÍTULO I, EL PROBLEMA contiene: Planteamiento del problema, Formulación del Problema, Objetivos del Estudio (General y Específicos), Justificación, Hipótesis y Delimitación del problema.

El CAPÍTULO II MARCO REFERENCIAL contiene: Antecedentes Históricos, Marco Contextual, Marco Conceptual, Marco Teórico y Marco Legal.

El CAPÍTULO III DISEÑO METODOLOGICO contiene: Tipo de Investigación, Población y Muestra, Técnicas e Instrumentos de Recolección de la Información y Análisis de la Información Recolectada.

El CAPÍTULO IV PRESENTACION DE RESULTADOS contiene: Diagnóstico del Área de Contabilidad de la E.S.E. Hospital Local de Rio de Oro Cesar, Identifica los elementos que conforman el SGSI – Sistema de Gestión de Seguridad de la Información para el Área de Contabilidad de la E.S.E y Documento formal para la Gestión de la Seguridad de la Información del Área de Contabilidad que incorpore la Política de la Seguridad de la Información

1. TITULO

Sistema de Gestión de Seguridad de la Información (SGSI) para el Área de Contabilidad de la E.S.E. Hospital Local De Rio De Oro Cesar.

1.1 PLANTEAMIENTO DEL PROBLEMA

En un mundo actual de constantes cambios tecnológicos, el manejo de la seguridad de información a todo nivel se convierte en un problema grave cuando no se le brinda el control y tratamiento apropiado.

Luego de analizar la infraestructura tecnológica del Área de Contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar, 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 disponibilidad, integridad y confiabilidad de la información, razón por la cual es necesario 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 de Contabilidad del Hospital, esto redundaría en pérdidas económicas y podría generar desconfianza sobre la imagen que mantiene la E.S.E en el medio de la salud.

1.2 FORMULACIÓN DEL PROBLEMA

¿Un Sistema de Gestión de Seguridad de la Información constituirá un mecanismo que le facilite al Área de Contabilidad de la E.S.E Hospital Local de Rio de Oro, regular, gestionar y mitigar los riesgos actuales asociados al uso de la información de los sistemas y servicios informáticos?

1.3 OBJETIVOS

1.3.1Objetivo general

Plantear un Sistema de Gestión de Seguridad de la Información (SGSI) para el Área de Contabilidad de la E.S.E. Hospital Local de Rio de Oro Cesar.

1.3.2Objetivos específicos

✓ Realizar un diagnóstico del Área de Contabilidad de la E.S.E. Hospital Local de Rio de Oro Cesar.

✓ Identificar los elementos que conforman el SGSI – Sistema de Gestión de Seguridad de la Información para el Área de Contabilidad de la E.S.E.

✓ Elaborar un documento formal para la gestión de la seguridad de la información del Área de contabilidad que incorpore la política de la seguridad de la información.

1.4JUSTIFICACIÓN

En muchas empresas la seguridad de la información es tratada como un problema solo tecnológico, sin tomar en cuenta que la seguridad de la información es un problema organizativo y de gestión, lo que con lleva a que las empresas no sean capaces de afrontar ataques provenientes de todos los ángulos.

La seguridad puede ser afectada a través de cualquiera de sus tres componentes: el uso indebido de la tecnología, la falta de procesos de planificación de seguridad o el desconocimiento de las personas acerca de las distintas medidas de seguridad informática.

Mediante un SGSI – Sistema de Gestión de Seguridad de la Información, el Área de Contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar conseguirá minimizar considerablemente el riesgo de que su productividad se vea afectada debido a la ocurrencia de un evento que comprometa la confidencialidad, disponibilidad e integridad de la información o de alguno de los sistemas informáticos. Este sistema permite identificar, gestionar y minimizar los riesgos reales y potenciales de la seguridad de la información, de una forma documentada, sistemática, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

1.5 HIPOTESIS

Con un Sistema de Gestión de Seguridad de la Información se logrará minimizar los factores de riesgo para el Área de contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar.

1.6 DELIMITACIONES

1.6.1 Geográficas. Este proyecto se desarrollará en el Área de Contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar.

1.6.2 Temporal. Este proyecto tendrá un tiempo de realización de 4 Meses, de acuerdo a las diferentes actividades a realizar durante el desarrollo del mismo.

1.6.3 Conceptual. Los conceptos que se van a manejar en este proyecto se van a relacionar con la Seguridad de la Información, Sistema de Gestión de Seguridad de la Información (SGSI), Riesgos, Administración de Riesgos, Políticas de Seguridad de la Información y Controles.

1.6.4 Operativa. Este proyecto diseñará un Sistema de Gestión de Seguridad de la Información (SGSI) para el Área de Contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar, buscando asegurar que la tecnología de información usada, esté alineada con la estrategia de negocio y que los activos de información tengan el nivel de protección acorde con el valor y riesgo que represente para la misma.

2. MARCO REFERENCIAL

2.1 ANTECEDENTES HISTÓRICOS

2.1.1 Implementación de un Sistema de Gestión de Seguridad de la Información basada en la norma ISO 27001. Para la Intranet de la Corporación Metropolitana de Salud. Flor María Álvarez Zurita y Pamela Anabel García Guzmán. Quito, Ecuador. 2007. El objetivo principal de este proyecto de investigación es la implementación de un Sistema de Gestión de Seguridad de la Información para la Intranet de la Corporación Metropolitana de Salud en base a la Norma ISO 27001 con el fin de lograr una gestión de la red de manera organizada, adecuada y garantizando que los riesgos de seguridad de la red sean minimizados en base a los procedimientos para el tratamiento de los mismos[1].

2.1.2 Plan de Gestión de Seguridad de la Información basado en TIC'S para la Facultad de Ingeniería de Sistemas de la Escuela Politécnica Nacional. Mireya Isabel Vasco Aguas y Mercedes Estefanía Verdezoto Saltos. Quito, Ecuador. 2009. **El plan constituye el establecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) que consiste en establecer la política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la Facultad, para ella se contempla los requerimientos de seguridad basándose en el estudio de los riesgos de seguridad y en la recopilación y estudio de los documentos organizacionales y legales para la selección de los objetivos de control y controles incluidos en los estándares ISO/IEC 27001:2005 e ISO/IEC 17799:2005[2].**

2.1.3 Centro de investigaciones económicas, administrativas y sociales. Gestión de la Seguridad de la Información en la Empresa. Oscar Raúl Ortega Pacheco. México, D.F. 2010. El presente documento presenta una serie de acciones aplicadas a un modelo de gestión de la seguridad de la información que permite alinear los objetivos de una empresa con las metas que se requieren para la protección de la información. Para lo cual partimos de la construcción de un modelo de gestión de la información que permite explicar el flujo completo que sufren los datos dentro de una empresa. Posteriormente se describen los diferentes modelos de gestión de riesgo informático donde se analizan sus principales ventajas y desventajas. Finalmente, partiendo de la base del modelo propuesto por Kiely y Benzel (2009) se establecen diferentes medidas que una empresa puede aplicar desde sus políticas, gobierno corporativo, elementos técnicos y de cultura para minimizar el riesgo

[1] ÁLVAREZ ZURITA, Flor M y GARCÍA GUZMÁN, Pamela A. Implementación de un Sistema de Gestión de Seguridad de la Información basada en la norma ISO 27001. Para la Intranet de la Corporación Metropolitana de Salud. Quito, Ecuador.. 2007. 298 h. Escuela Politécnica Nacional. [en línea]. http://bibdigital.epn.edu.ec/handle/15000/565

[2] VASCO AGUAS, Mireya I y VERDEZOTO SALTOS, Mercedes E. Plan de Gestión de Seguridad de la Información basado en TIC'S para la Facultad de Ingeniería de Sistemas de la Escuela Politécnica Nacional. Quito, Ecuador.. 2009. 226 h. Escuela Politécnica Nacional. [en línea]. http://bibdigital.epn.edu.ec/handle/15000/4370?mode=full

informático. Así mismo se sugiere trabajar a futuro en la construcción de indicadores de seguridad, evaluar la validez del modelo presentado ante nuevos retos tecnológicos y desarrollar estudios de trayectoria tecnológica en cuanto a delitos electrónicos como innovación en elementos de seguridad[3].

2.1.4 Plan de Propuesta para la Implantación de la Norma de Seguridad Informática ISO 27001:2005, para el Grupo Social Fondo Ecuatoriano Populorum Progressio (GSFEPP). Oscar Eduardo Campaña Tenesaca. Quito, Ecuador. 2010. Implantar un Sistema de Gestión de Seguridad de la Información (SGSI), es de mucha ayuda para entidades que basan su sostenibilidad en la claridad y respaldo de la información que esta genera en el aspecto de manejo financiero y de proyectos, ya que así seguirán recibiendo financiamiento de entidades extranjeras, pero las dificultades aparecen duramente la explicación del proceso de análisis de riesgos y vulnerabilidades y se intensifican con la necesidad de colaboración de una parte importante de las personas de la empresa con la dirección al frente, esto se debe a la cultura poco participativa de nuestra sociedad[4].

2.1.5 Sistema de Gestión de Seguridad de la Información para una Institución Financiera. Moises Antonio Villena Aguilar. Lima, Perú. 2006. La presente tesis ha realizado una investigación de las normas y estándares que van difundiéndose con mayor énfasis en el mercado peruano, en especial en el sector financiero. Se rescataron los aspectos más saltantes de cada norma y estándar, a partir de los cuales se plantea un esquema de gestión de seguridad de información que puede ser empleado por una institución financiera en el Perú, lo cual permitirá que ésta con las normas de regulación vigentes en lo relacionado a la Seguridad de Información[5].

2.1.6 Desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) para la empresa Comware S.A. en la ciudad de Quito, aplicando la norma ISO/IEC 27001. Diego Calderón y David Sánchez. Quito, Ecuador. 2012. El presente proyecto de titulación tiene como objetivo el diseño de un Sistema de Gestión de Seguridad de la Información para la empresa Comware S.A. en la ciudad de Quito basado en la Norma ISO 27001, con el fin de lograr un esquema que sirva como guía para la posterior implementación y certificación de la Norma en la empresa. Se realizó un análisis por medio de varios software que permitieron ver algunas falencias dentro de los sistemas que se

[3] ORTEGA PACHECO, Oscar R. Centro de investigaciones económicas, administrativas y sociales, Gestión de la Seguridad de la Información en la Empresa. México D.F. 2010. 90h. Instituto Politécnico Nacional. [en línea]. http://www.repositoriodigital.ipn.mx/handle/123456789/6564

[4] CAMPAÑA TENESACA, Oscar E. Plan de Propuesta para la Implantación de la Norma de Seguridad Informática ISO 27001:2005, para el Grupo Social Fondo Ecuatoriano Populorum Progressio (GSFEPP). Quito, Ecuador. 2010. 207h. [en línea] http://dspace.ups.edu.ec/handle/123456789/4468?mode=full

[5] VILLENA AGUILAR, Moises A. Sistema de Gestión de Seguridad de la Información para una Institución Financiera. Lima, Perú. 2006. 72h. Pontificia Universidad Católica del Perú. [en línea] http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/362/VILLENA_MOIS%C3%89S_SISTEMA_DE%20GESTI%C3%93N_DE_SEGURIDAD_DE_INFORMACI%C3%93N_PARA_UNA_INSTITUCI%C3%93N_FINANCIERA.pdf

manejan en la empresa y de esta forma realizar un análisis de las amenazas que se encuentran latentes en los sistemas informáticos[6].

2.2 MARCO CONTEXTUAL

El desarrollo de la investigación se llevara a cabo en el Área de Contabilidad de la E.S.E. Hospital Local de Rio de Oro Cesar, en el municipio de Rio de Oro, Cesar Colombia, donde se estudiará el modelo del negocio de los procesos del Área y se realizará el diseño del Sistema de Gestión de Seguridad de la Información.

2.3 MARCO CONCEPTUAL

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

2.3.1 Administración de riesgos. Se llama así al proceso de identificación, análisis y evaluación de riesgos[7].

2.3.2 Control. El control es un proceso por el cual la administración verifica si lo que ocurre concuerda con lo que supuestamente debe ocurrir. Permite que se realicen los ajustes o correcciones necesarias en caso se detectan 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[8].

2.3.3 Declaración de aplicabilidad. La declaración de aplicabilidad o SOA, del inglés Statement of Applicability, es un documento que se referencia en la cláusula 4.2.1 del estándar ISO/IEC 27001 y 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[9].

---

[6] CALDERÓN, Diego y SÁNCHEZ, David. Desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) para la empresa Comware S.A. en la ciudad de Quito, aplicando la norma ISO/IEC 27001. Quito, Ecuador. 2012. 216h. Universidad Politécnica Salesiana. [en línea] https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCwQFjAA&url=http%3A%2F%2Fdspace.ups.edu.ec%2Fbitstream%2F123456789%2F3901%2F1%2FUPS-ST000906.pdf&ei=GDsSUrOEJaao2wWI7YCYAQ&usg=AFQjCNFsKFoVxj06G_YJYJx906JAEUBptQ&sig2=CxONXw8ZwdZkaOorjVnyxw&bvm=bv.50768961,d.b2I

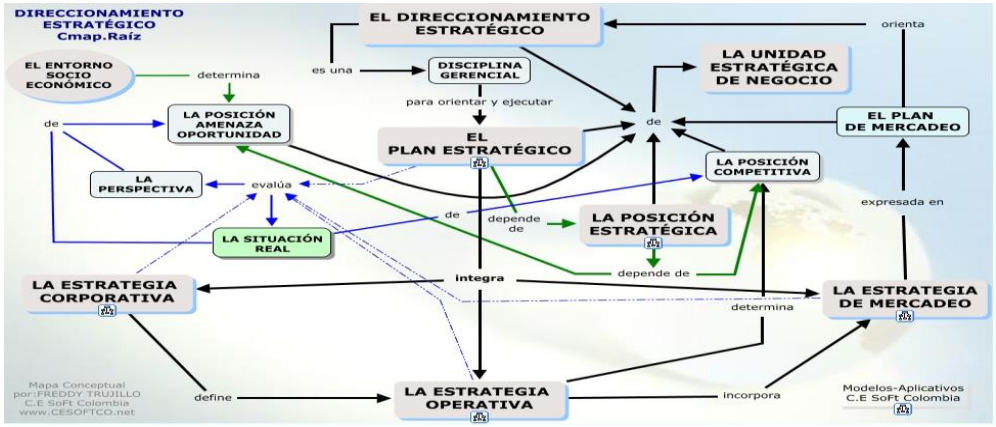
[7] ADMINISTRACIÓN DE RIESGOS. AS/NZS 4360:2004

[8] INTERNATIONAL STANDARD ISO/IEC 17799:2005. Iso-Iec 17799:2005.pdf. 2005

[9] INTERNATIONAL ORGANIZATION FOR STANDARIZATION ISO/IEC 27000. www.iso27000.es. 2008

2.3.4 Direccionamiento Estratégico. El "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 estrategias fundamentales e interrelacionadas: a) La Estrategia Corporativa, b) La Estrategia de Mercadeo y c) La Estrategia Operativa o de Competitividad[10].

Figura 1. Direccionamiento estratégico



Fuente: TRUJILLLO, Freddy.

El Direccionamiento Estratégico podríamos definirlo como el instrumento metodológico por el cual establecemos los logros esperados y los indicadores para controlar, identificamos los procesos críticos dentro de la gestión, los enfoques, y demás áreas importantes que tengan concordancia con la misión, la visión, y los objetivos establecidos.

En otras palabras, el Direccionamiento Estratégico lo podemos considerar como la materia prima o insumo fundamental para aplicar la Planeación Estratégica, Táctica y Operativa que al final dicha aplicación es la que nos garantiza el poder alcanzar el lugar el cual nos hemos propuesto[11].

La planeación estratégica es el proceso mediante el cual quienes toman decisiones en una organización obtienen, procesan y analizan información pertinente, interna y externa, con el fin de evaluar la situación presente de la empresa, así como su nivel de competitividad con

[10] TRUJILLLO, Freddy. C.E Soft Colombia. [En línea] [Citado el: 28 de enero de 2013.] http://cesoftco.net/2cmc/PAPER.htm.
[11] BELTRAN, Gustavo. Consultoría Estratégica y coachig de negocios. [En línea] [Citado el: 28 de 01 de 2013.] http://gustavobeltran.com/%C2%BFque-se-entiende-por-direccionamiento-estrategico/.

el propósito de anticipar y decidir sobre el direccionamiento de la institución hacia el futuro[12].

2.3.5 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.

2.3.6 Información. Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. 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.

2.3.7 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 requieras[13].

2.3.8 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[14].

2.3.8 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.

2.3.9 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.

2.4 MARCO TEÓRICO

Con el pasar de los años la seguridad de información ha tomado una mayor importancia, lo que trajo consigo que un grupo de especialistas a nivel mundial en temas relacionados a seguridad, riesgos y temas afines, desarrollen diversos marcos de trabajo, metodologías, estándares, buenas prácticas, distintos modelos para diseñar un SGSI, leyes, normativas, entre otros, con la finalidad de brindar a las empresas la oportunidad de adoptarlas y proteger adecuadamente la información de sus clientes.

[12] GÓMEZ, Humberto. Gerencia Estratégica Planeación y Gestión - Teoría y metodología. Santa Fé de Bogotá : 3R Editores, 1994.
[13] RFC 1244: Site Security Handbook. J. Reynolds – P. Holbrook. Julio 1991
[14] ADMINISTRACIÓN DE RIESGOS. AS/NZS 4360:2004

2.4.1 ISO/IEC 27001:2005[15]

Este estándar internacional ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización.

En función del tamaño y necesidades se implementa un SGSI con medidas de seguridad más o menos estrictas, que en cualquier caso pueden variar a lo largo del tiempo.

2.4.2 Enfoque del proceso. Una organización necesita identificar y manejar muchas actividades para poder funcionar de manera efectiva. Cualquier actividad que usa recursos y es manejada para permitir la transformación de éstos en outputs, se puede considerar un proceso.

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación y las interacciones de estos procesos, y su gestión, puede considerarse un enfoque del proceso.

El enfoque del proceso para la gestión de la seguridad de la información que presenta este estándar internacional fomenta que sus usuarios enfaticen la importancia de:

- Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
- Implementar y operar controles para manejar los riesgos de la seguridad de la información.
- Monitorizar y revisar el desempeño y la efectividad del SGSI.
- Mejora continua en base a la medición del objetivo.

Este estándar Internacional adopta el modelo del proceso Planificar-Hacer-Comprobar-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI.

La figura muestra como un SGSI toma como entrada los requerimientos y expectativas de la seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que satisfacer aquellos requerimientos y expectativas.

[15] INTERNATIONAL ORGANIZATION FOR STANDARIZATION ISO/IEC 27000. www.iso27000.es. 2008

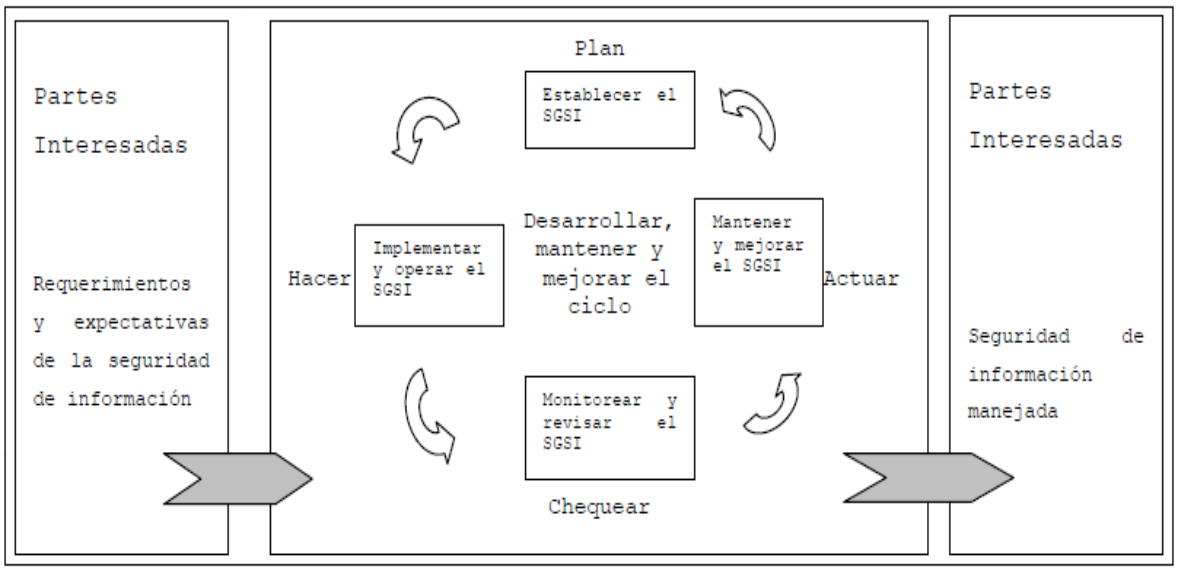


Figura 2. Modelo PDCA aplicado a los procesos SGSI

La siguiente tabla muestra en profundidad una descripción de las acciones llevadas a cabo en cada uno de los estados del modelo PDCA.

Tabla 1. Acciones realizadas en el modelo PDCA.

Estado	Acciones
Planificar (establecer el SGSI)	Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.
(Implementar y utilizar el SGSI)	Implementar y utilizar la política, controles, procesos y procedimientos SGSI.
Comprobar (Monitorizar y revisar el SGSI)	Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias practicas del SGSI e informar de los resultados a la gerencia para su revisión.
Actuar (Mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr la mejora continua del SGSI.

2.4.3 Compatibilidad con otros sistemas de gestión. Este estándar internacional es compatible con el ISO 9001:2000 e ISO 14001:2004 para dar soporte a una implementación y operación consistente e integrada con los estándares de gestión relacionados. Por lo tanto, un sistema de gestión adecuadamente diseñado puede satisfacer los requerimientos de todos estos estándares.

Además se puede utilizar en conjunción con el estándar ISO/IEC 27002 que proporciona un modelo contrastado para la implementación de los controles de seguridad.

Aplicación

Los requerimientos establecidos en este Estándar Internacional son genéricos y están diseñados para ser aplicables a todas las organizaciones, sin importar el tipo, tamaño y naturaleza. No es aceptable la exclusión de ninguno de los requerimientos especificados en las Cláusulas 4, 5, 6 y 8 cuando una organización asegura su conformidad con este Estándar Internacional.

Cualquiera exclusión de los controles vista como necesaria para satisfacer el criterio de aceptación del riesgo tiene que ser justificada y se debe proporcionar evidencia de que los riesgos asociados han sido aceptados por las personas responsables. Cuando se realizan exclusiones, las aseveraciones de conformidad con este estándar no son aceptables a no ser que estas exclusiones no afecten la capacidad y/o responsabilidad de la organización, para proporcionar seguridad de la información que satisfaga los requerimientos de seguridad determinados por la evaluación de riesgo y los requerimientos reguladores aplicables.

Nota: Si una organización ya cuenta con un sistema de gestión de procesos comerciales operativos (por ejemplo, en relación con ISO 9001 o ISO 14001), en la mayoría de los casos es preferible satisfacer los requerimientos de este Estándar Internacional dentro de este sistema de gestión existente.

2.4.4 ISO/IEC 27002:2005

Describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 11 dominios, mencionados en el anexo A de la ISO 27001, 39 objetivos de control y 133 controles.

Los dominios a tratar son los siguientes:

- **Políticas de Seguridad:** Busca establecer reglas para proporcionar la dirección gerencial y el soporte para la seguridad de la información. Es la base del SGSI.

- **Organización de la seguridad de la información:** Busca administrar la seguridad dentro de la compañía, así como mantener la seguridad de la infraestructura de procesamiento de la información y de los activos que son accedidos por terceros.

- **Gestión de activos:** Busca proteger los activos de información, controlando el acceso solo a las personas que tienen permiso de acceder a los mismos. Trata que cuenten con un nivel adecuado de seguridad.

- **Seguridad de los recursos humanos:** Orientado a reducir el error humano, ya que en temas de seguridad, el usuario es considerado como el eslabón más vulnerable y por el cual se dan los principales casos relacionados con seguridad de la información. Busca capacitar al personal para que puedan seguir la política de seguridad definida, y reducir al mínimo el daño por incidentes y mal funcionamiento de la seguridad.

- **Seguridad física y ambiental:** Trata principalmente de prevenir el acceso no autorizado a las instalaciones para prevenir daños o pérdidas de activos o hurto de información.

- **Gestión de comunicaciones y operaciones:** Esta sección busca asegurar la operación correcta de los equipos, así como la seguridad cuando la información se transfiere a través de las redes, previniendo la pérdida, modificación o el uso erróneo de la información.

- **Control de accesos:** El objetivo de esta sección es básicamente controlar el acceso a la información, así como el acceso no autorizado a los sistemas de información y computadoras. De igual forma, detecta actividades no autorizadas.

- **Sistemas de información, adquisición, desarrollo y mantenimiento:** Básicamente busca garantizar la seguridad de los sistemas operativos, garantizar que los proyectos de TI y el soporte se den de manera segura y mantener la seguridad de las aplicaciones y la información que se maneja en ellas.

- **Gestión de incidentes de seguridad de la información:** Tiene que ver con todo lo relativo a incidentes de seguridad. Busca que se disponga de una metodología de administración de incidentes, que es básicamente definir de forma clara pasos, acciones, responsabilidades, funciones y medidas correctas.

- **Gestión de continuidad del negocio:** Lo que considera este control es que la seguridad de la información se encuentre incluida en la administración de la continuidad de negocio. Busca a su vez, contrarrestar interrupciones de las actividades y proteger los procesos críticos como consecuencias de fallas o desastres.

- **Cumplimiento:** Busca que las empresa cumpla estrictamente con las bases legales del país, evitando cualquier incumplimiento de alguna ley civil o penal, alguna obligación reguladora o requerimiento de seguridad.
A su vez, asegura la conformidad de los sistemas con políticas de seguridad y estándares de la organización.

2.4.5 COBIT 4.1[16]

COBIT es un framework (también llamado marco de trabajo) de Gobierno de TI y un conjunto de herramientas de soporte para el gobierno de TI que les permite a los gerentes cubrir la brecha entre los requerimientos de control, los aspectos técnicos y riesgos de negocio.

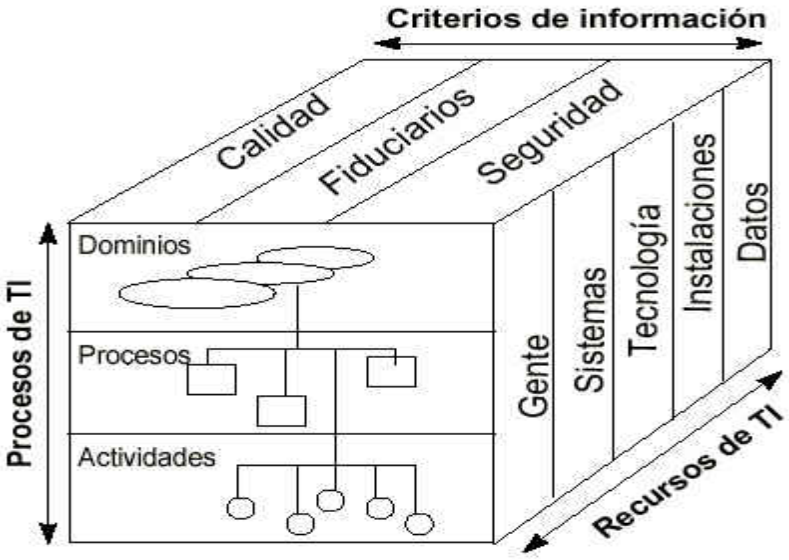
Describe como los procesos de TI entregan la información que el negocio necesita para lograr sus objetivos. Para controlar la entrega, COBIT provee tres componentes claves, cada uno formando una dimensión del cubo COBIT, que se puede apreciar en la Figura 2.

Como un framework de gobierno y control de TI, COBIT se enfoca en dos áreas claves:

- Proveer la información requerida para soportar los objetivos y requerimientos del negocio.

- Tratamiento de información como resultado de la aplicación combinada de recursos de TI que necesita ser administrada por los procesos de TI.

Figura 3. Cubo de COBIT

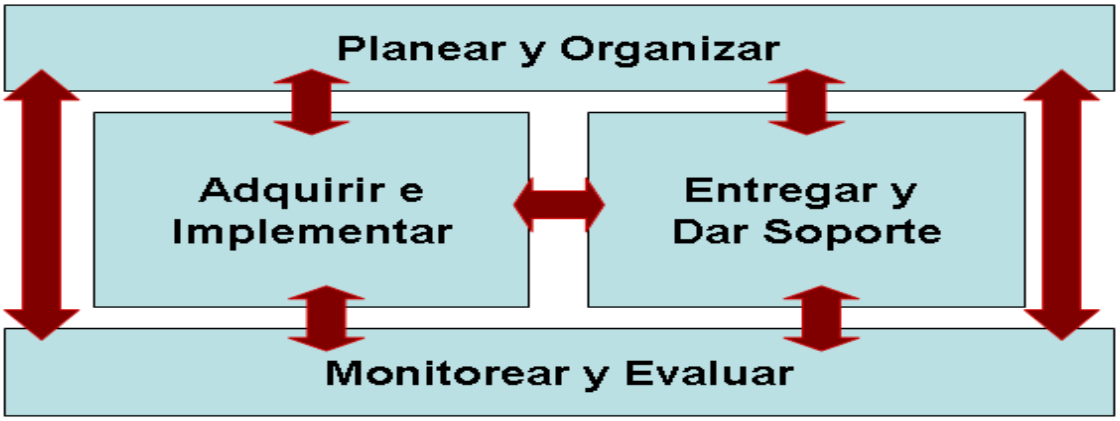


Fuente: COBIT 4.1, www.isaca.org

Tiene 34 procesos de alto nivel clasificados en cuatro dominios: Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte, y, Monitorear y Evaluar, tal y como se puede apreciar en la Figura 3.

[16] IT GOVERNANCE INSTITUTE. Cobit4.1.pdf. [en línea] http://www.isaca.org

Figura 4. Dominios de COBIT



Fuente: COBIT 4.1, www.isaca.org

La misión de COBIT es "investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información que sean autorizados (dados por alguien con autoridad), actualizados, e internacionales para el uso del día a día de los gestores de negocios (también directivos) y auditores."

COBIT brinda buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica, y están más enfocadas al control y mucho menos en la ejecución. El modelo COBIT cuenta con 4 dominios, 34 procesos de TI, 210 objetivos de control y 40 guías de auditoría. Los 4 dominios de COBIT son:

- **Planear y Organizar:** Este dominio cubre las estrategias y se refiere a la forma en que la tecnología de información puede contribuir a que se cumplan los objetivos del negocio. Busca establecer una organización y una infraestructura tecnológica apropiadas. Los procesos de TI con los que cuenta este dominio son:

- Definir un Plan Estratégico de TI
- Definir la Arquitectura de la Información
- Determinar la Dirección Tecnológica
- Definir los Procesos, Organización y Relaciones de TI
- Administrar la Inversión en TI
- Comunicar las Aspiraciones y la Dirección de la Gerencia
- Administrar Recursos Humanos de TI
- Administrar la Calidad
- Evaluar y Administrar los Riesgos de TI
- Administrar Proyectos

- **Adquirir e Implementar:** Las soluciones deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio para llevar a cabo la estrategia de TI.

Este dominio cubre los cambios y el mantenimiento realizado a sistemas existentes. Los procesos de TI con los que cuenta este dominio son:

- Identificar soluciones automatizadas.
- Adquirir y mantener software aplicativo.
- Adquirir y mantener infraestructura tecnológica.
- Facilitar la operación y el uso.
- Adquirir recursos de TI.
- Administrar cambios.
- Instalar y acreditar soluciones y cambios.

- **Entregar y Dar Soporte:** Este dominio hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, seguridad y continuidad. Incluye el procesamiento de los datos por sistemas de aplicación, clasificados frecuentemente como controles de aplicación. Los procesos de TI con los que cuenta este dominio son:

- Definir y administrar los niveles de servicio.
- Administrar los servicios de terceros.
- Administrar el desempeño y la capacidad.
- Garantizar la continuidad del servicio.
- Garantizar la seguridad de los sistemas.
- Identificar y asignar costos.
- Educar y entrenar a los usuarios.
- Administrar la mesa de servicio y los incidentes.
- Administrar la configuración.
- Administrar los problemas.
- Administrar los datos.
- Administrar el ambiente físico.
- Administrar las operaciones.

- **Monitorear y Evaluar:** Este dominio hace hincapié a que los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control. Los procesos de TI con los que cuenta este dominio son:

- Monitorear y evaluar el desempeño de TI.
- Monitorear y evaluar el Control interno.
- Garantizar el cumplimiento regulatorio.
- Proporcionar el gobierno de TI.

COBIT a su vez, tiene 7 criterios de información, agrupados en 3 requerimientos (calidad, fiduciarios y seguridad) con los que clasifica a cada uno de los 34 procesos de TI, según el enfoque que tenga el proceso. Estos criterios son:

- Efectividad: Se refiere a la información cuando es entregada de manera correcta, oportuna, consistente y usable.

- Eficiencia: Se refiere a la provisión de información a través de la utilización óptima de los recursos.

- Confidencialidad: Se refiere a la protección de la información sensible de su revelación no autorizada. Tiene que ver que con la información enviada a una persona debe ser vista solo por esa persona y no por terceros.

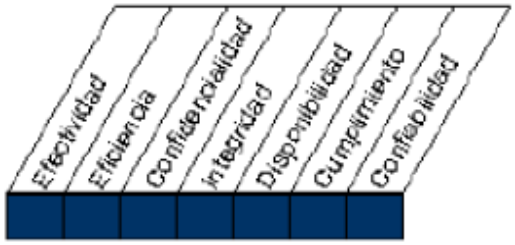
- Integridad: Se refiere a que la información no haya sufrido cambios no autorizados.

- Disponibilidad: Se refiere a que la información debe estar disponible para aquellas personas que deban acceder a ella, cuando sea requerida.

- Cumplimiento: Se refiere a cumplir con las leyes, regulaciones y acuerdos contractuales a los que la compañía se encuentra ligada.
- Confiabilidad: Se refiere a la provisión de la información apropiada a la alta gerencia que apoyen a la toma de decisiones.

En todos los procesos de TI del COBIT se puede saber a qué enfoque está orientado. Puede ser que abarque todos los enfoques, o que sólo abarque algunos, y para todos los controles se indicará si el enfoque es primario (P) o secundario (S).

Figura 5. Enfoque de procesos de TI de COBIT



Fuente: COBIT 4.1, www.isaca.org

Con respecto a los recursos de TI mencionados en la otra dimensión del cubo, se definen de la siguiente manera:

- Aplicaciones: Son procedimientos manuales y sistemas de usuarios automatizados que procesan información.

- Información: Es data que son ingresada, procesada y obtenida de los sistemas de información en cualquier formato usado por el negocio.

- Infraestructura: Incluye la tecnología y facilidades tales como: hardware, sistemas operativos y redes que permiten el procesamiento de las aplicaciones.

Personas: Son requeridos para planificar, organizar, adquirir, implantar, entregar, soportar, monitorear y evaluar los servicios y sistemas de información. Ellos podrían ser internos, outsourcing o contratado

2.5 MARCO LEGAL

2.5.1 Constitución Política de 1991. En los artículos 209 y 269 se fundamenta el sistema de control interno en el Estado Colombiano, el primero establece: "La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley" y en el 269, se soporta el diseño del sistema: "En las entidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley, la cual podrá establecer excepciones y autorizar la contratación de dichos servicios con empresas privadas colombianas".

2.5.2 Leyes informáticas colombianas[17]

Ley estatutaria 1266 del 31 de diciembre de 2008

Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 del 5 de enero de 2009. Delitos informáticos

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.

[17] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Gerencia de Innovación y Desarrollo Tecnológico. Última actualización el Lunes, 22 de Abril de 2013 09:05. [en línea]. http://www.unad.edu.co/gidt/index.php/leyesinformaticas

Ley 1341 del 30 de julio de 2009

Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Ley estatutaria 1581 de 2012

Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

Aspectos claves de la normatividad:

1. Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.

2. Establece los principios que deben ser obligatoriamente observados por quienes hagan uso, de alguna manera realicen el tratamiento o mantengan una base de datos con información personal, cualquiera que sea su finalidad.

3. Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben presentar si son públicos o privados, así como las finalidades permitidas para su utilización.

4. Crea una especial protección a los datos de menores de edad.

5. Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante.

6. Define las obligaciones y responsabilidades que empresas de servicios tercerizados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.

7. Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia Delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.

8. Crea el Registro Nacional de Bases de Datos.

9. Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos.

2.5.3 Ley 603 de 2000. Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

2.5.4 El derecho de autor[18]Constitución Política de 1991. En su artículo 61, que expresa: "El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley".

Decisión 351 de 1993, o Régimen Común Andino sobre Derecho de Autor y Derechos Conexos, es de aplicación directa y preferente a las leyes internas de cada país miembro del Grupo Andino.

Ley 23 de 1982, contiene las disposiciones generales y especiales que regulan la protección del derecho de autor en Colombia.

Ley 44 de 1993 (febrero 15), modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944.

DECRETO 1360 DE 1989 (junio 23). "Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor".

Decreto 460 de 1995, por la cual se reglamenta el Registro Nacional de Derecho de Autor.

DECRETO 1474 DE 2002 (Julio 15). "Por el cual se promulga 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)".

2.5.5 Ley 734 de 2002, Numeral 21 y 22 del Art. 34, son deberes de los servidores Públicos "vigilar y salvaguardar los bienes y valores que le han sido encomendados y cuidar que sean utilizados debida y racionalmente", y "responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización"[19]

[18] MINISTERIO DEL INTERIOR Y DE JUSTICIA DE COLOMBIA. Dirección Nacional del Derecho de Autor. Unidad Administrativa Especial. [en línea]. http://www.propiedadintelectualcolombia.com/Site/LinkClick.aspx?fileticket=yDsveWsCdGE%3D&tabid=

[19] SUPERINTENDENCIAS DE SOCIEDADES. Manual Manejo y Control Administrativo de los Bienes de Propiedad. Bogotá D.C., Colombia, 2009. 29h. [en línea].

2.5.6 DECRETO 1377 DE 2013. Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012.

http://www.supersociedades.gov.co/web/Ntrabajo/SISTEMA_INTEGRADO/Documentos%20Infraestructura/DOCUMENTOS/GINF-M-001%20MANUAL%20ADMINISTRATIVO.pdf

3. DISEÑO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

En este proyecto se utilizarán diferentes tipos de estudio o investigación, entre estos tenemos:

3.1.1 Tipo de investigación descriptiva. Esta investigación detalla en forma breve y especifica los componentes de la investigación permitiendo comprobar en forma sistemática y progresiva las necesidades de la entidad objeto de estudio.

3.1.2 Tipo de investigación explicativa. Este proyecto utilizará investigación explicativa pues a través del proceso de investigación, intenta establecer las causas de los eventos objeto de este estudio, mediante el análisis de la situación actual queda claramente explicita la necesidad de normalizar los controles en lo referente a la seguridad de la información.

3.1.3 Tipo de investigación de campo. Esta investigación es de campo pues se apoya en información obtenida mediante entrevistas, reuniones, listas de chequeo, encuestas, observación y asesoramiento técnico.

3.2 POBLACIÓN

Según Tamayo y Tamayo, ¨La población se define como la totalidad del fenómeno a estudiar donde las unidades de población poseen una característica común la cual se estudia y da origen a los datos de la investigación¨.

La población que se tendrá en cuenta para la realización de esta investigación está conformada por la Gerencia y Área de contabilidad.

3.3 MUESTRA

Tamayo y Tamayo, afirma que la muestra ¨es el grupo de individuos que se toma de la población, para estudiar un fenómeno estadístico¨.

Para el desarrollo de esta investigación se toma como muestra el Gerente, el Contador, el Auxiliar Contable, la encargada de Facturación.

3.4 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Durante el desarrollo de este proyecto se utilizaran los métodos de investigación inductiva y deductiva.

Podemos decir que se utilizará el método inductivo deductivo, pues ayuda a la identificación o determinación de que controles o aspectos de las diferentes Normas y

Estándares son aplicables al Área de Contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar, así como descartar aquellos que no sean necesarios.

Además se aplicarán las siguientes técnicas de recolección de información:

- Observación
- Entrevistas
- Revisión documental
- Encuestas
- Listas de chequeo

3.5 ANÁLISIS DE INFORMACIÓN

Durante el desarrollo de este proyecto se recopilará información relacionada con el uso de tecnologías de información dentro del Área de Contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar, se realizará 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.

La información recaudada, se analizará cualitativamente, donde se determinarán aspectos relacionados con el proyecto, estableciendo así un diagnóstico, para lo cual se espera la veracidad por parte de las personas entrevistadas.

Encuesta – auditoria Administrativa – área de contabilidad
Nombre de la Empresa: ESE Hospital Local de Rio de Oro Cesar

ENCUESTA		
Objetivo: recopilar información para evaluar administrativamente y los sistemas de información del área contable de la ESE Hospital Local de Rio de Oro cesar		
Nombre del encuestado	**Cargo del encuestado**	**Teléfono del encuetado:**
Carlos Fernando Lemus	Jefe Administrativo Y Financiero	3128761238

Auditoria Administrativa al área Contable de la ESE Hospital Local de Rio de Oro cesar	**Calificar el grado de cumplimiento**	
Preguntas	**SI**	**NO**
Conoce la misión, visión. Valores y principios de la ESE	x	
Cuenta con un objetivo definido para la realización de su trabajo en el área contable de la ESE?	x	
¿Sabe usted si la empresa cuenta con unidades de medida para cuantificar el avance de sus acciones?		x
¿Cuenta con un programa de trabajo?		x
¿Están claramente delimitadas sus funciones?	x	
¿Existe duplicidad de funciones?		

¿El ambiente laboral de la empresa es bueno?	x	
¿El ambiente laboral de la empresa es Malo?		x
Tiene indicadores para medir el proceso del área contable		
Se realizan evaluaciones contables		x
Los actividades del área contable se encuentran bien definidos		x

LISTA DE CHEQUEO – auditoria Administrativa – área de contabilidad
Nombre de la Empresa: ESE Hospital Local de Rio de Oro Cesar
Fecha: 14 de Julio de 2013 a 14 de agosto de 2013

Evaluar el funcionamiento administrativo del área contable de la ESE Hospital Local de Rio de Oro Cesar	
Descripción de Concepto	**Cumple**
La ESE Hospital Local de Rio de Oro tiene definido la misión, visión, principios y calores del área contable?	si
La misión, visión. Principios y valores del área contable de la ese se pueden medir?	si
Los objetivos del área contable se han definido con los objetivos generales de la ESE	si
Se han definido Factores Claves de éxitos para lograr los objetivos propuestos en la ESE	si
Se definieron indicadores para verificar el cumplimiento de los objetivos	no
La ESE tiene definida políticas sobre el riesgo y controles en los niveles de operaciones del área contable y están modificadas de acuerdo a las necesidades	no
Se vigila el ambiente interno del área contable dentro de la ESE	no
Los impactos financiero son calificados periódicamente	no
Está definido el nivel de autoridad	no
Se han implementado canales de comunicación efectivos	
Se mide el rendimiento de la organización	no
Existe un plan de recurso humano alineado con los objetivos y las estrategias de la ESE	no
El área cuenta con procedimientos que le permitan identificar las necesidades de capacitación de sus empleados teniendo en cuenta los objetivos	no
El desempeño de los empleados es medido por lo menos una vez al año	no
Se monitorea el clima organizacional	no
Existen planes de crecimiento dentro de la ESE para los empleados	no
Se promueve la satisfacción de los empleados	no
Están identificados los riesgos que impidan el logro de los objetivos en el área contable	no
Se mide el rendimiento del proceso contable, costos, calidad, tiempos.	no

Las actividades de control en el área contable se vigilan de forma permanente	no
Los procesos en el área contable están documentados y se revisan de forma permanente para actualizarlos y mejorarlos	no
Existen canales de comunicación donde los que interviene en el proceso contable den sus sugerencias para el mejoramiento del proceso	no
Las reciben las quejas y se les hace tratamiento referentes al proceso contable	no
Se han desarrollado programas de mejoramiento continuo de la Calidad	no

LISTA DE CHEQUEO – auditoria Sistemas de Información – área de contabilidad
Nombre de la Empresa: ESE Hospital Local de Rio de Oro Cesar
Fecha: 14 de Julio de 2013 a 14 de agosto de 2013

Evaluar el funcionamiento de los sistemas de información del área contable de la ESE Hospital Local de Rio de Oro Cesar	
Descripción de Concepto	**Cumple**
Seguridad en la protección y conservación de locales, instalaciones, mobiliario y equipos	
Las condiciones generales de trabajo de los sistema computacionales del área contable son cómodas para el usuario del sistema	si
Tiene protección contra la humedad en el ambiente	no
Toman medidas para prevenir que los sistemas computacionales y las instalaciones eléctricas, telefónicas del área contable tengan contacto con el agua	no
Tienen protección contra partículas de polvo desechos volátiles de cualquier tipo a fin de evitar desperfectos en los sistemas computacionales en el are contable de la ESE	no
Tiene análisis de los sistemas de acomodación y pisos falsos	no
Análisis de regulación de temperatura y aire acondicionado	no
Análisis de regulación de la humead en el medio ambiente del área contable	no
Análisis de suministros de energía, comunicación y procesamiento de los datos	no
Análisis de limpieza del área contable	no
La iluminación artificial del área Contable y la iluminación por medio de luz solar.	no
Las instalaciones eléctricas, de datos y de comunicación	no
Los accesos y salidas en las áreas contable	si
La repercusión de los aspectos de carácter ergonómico.	no
Las adaptaciones de los equipos de cómputo.	si
Las condiciones de trabajo con computadora.	si

Protección contra contingencias causadas por la temperatura del sistema de aire acondicionado.	si
La ventilación natural de las áreas y espacios	si
Seguridad en la información del Área contable y bases de datos	
El rendimiento y uso del sistema computacional y de sus periféricos asociados es adecuado	no
La existencia, protección y periodicidad de los respaldos de bases de datos, software e información importante del área contable está bien definida.	no
La configuración, instalaciones y seguridad del equipo de cómputo, mobiliario y demás equipos del área de contable se encuentran de una forma adecuada y protegen la información	no
El rendimiento, la aplicación y la utilidad del equipo de cómputo, mobiliario y demás equipos del área contable son los adecuados	no
Evaluar la seguridad en el procesamiento de información.	no
Evaluar los procedimientos de captura, procesamiento de datos y emisión de resultados de los sistemas computacionales	no
Evaluar el estado físico de los sistemas	no

4. PRESENTACIÓN DE RESULTADOS

4.1 RECONOCIMIENTO DEL ÁREA DE CONTABILIDAD DE LA E.S.E HOSPITAL LOCAL DE RIO DE ORO CESAR.

4.1.1 DIRECCIONAMIENTO ESTRATÉGICO

4.1.1.1 Aspectos básicos de la E.S.E.

Nombre: Hospital Local de Río de Oro – Cesar
Gerente: Isaac Rafael Cervantes Barrios.
Ubicación Geográfica: Municipio de Río de Oro
Dirección: Avenida Araujo Cotes Cll 1ª # 3 - 24
Teléfono: 0975-619073 FAX 5619519
Email: hosprio@hotmail.com

4.1.1.2 Misión. La Empresa Social del Estado Hospital Local de Rio de Oro Cesar, tiene como misión integrar los servicios de primer nivel de atención de salud, con actitud humanizada, ética de calidad, promoviendo en nuestro quehacer diario, del crecimiento de talento humano, el desarrollo empresarial y la rentabilidad social a toda la población de río de oro.

4.1.1.3 Visión. La Empresa Social del Estado Hospital Local de Rio de Oro Cesar, será la empresa líder en la prestación de servicios médicos de primer nivel de atención (PNA), de mayor complejidad en la región, desarrollando un sistema de garantía de calidad, generando bienestar social a nuestros usuarios anticipando y respondiendo a los cambios de entorno para convertirlos en oportunidades.

4.1.1.4 Reseña Histórica. El centro materno infantil de salud de Río de oro-cesar fue transformado a la empresa social del estado HOSPITAL LOCAL de primer nivel de salud, mediante acuerdo N°033 de diciembre 02 de 1996, mediante sesión del honorable concejo municipal de Río de oro, departamento del cesar.

Una empresa social del estado de categoría especial de entidad pública con calidad descentralizada del orden municipal, dotada de personería jurídica, patrimonio propio y autonomía administrativa sometida al régimen jurídico previsto en el capítulo III articulo195 de la ley de 1993.

Su objetivo principal es la prestación de servicio de salud, entendido como un servicio público a carga del estado y como parte integrante del sistema de la seguridad social en salud, apoyando el desarrollo social de la región del cesar, mejorando la calidad de vida de los habitantes Rió dórense, en los índices de morbilidad, mortalidad, proveyendo la incapacidad y evitando el deterioro moral de los usuarios del servicios de salud.
La calidad de nuestros servicios objetivos como empresa social del estado hospital local de primer nivel de salud, es producir servicios de salud, eficientes y efectivos, que cumplan

con las normas de calidad establecidas de acuerdo con la reglamentación expedida para tal propósito.

Las prestación de los servicios de salud a la población que lo requiera, satisfaciendo los requerimiento del entorno con un adecuado y continuo de servicio en funcionamiento las 24 horas, en el servicio de salud, supervisando con el cumplimiento de los planes, programas y proyecciones definidos en las diversas áreas de la comunidad garantizando un excelente manejo gerencial adecuado con la rentabilidad social y financiera de la empresa.

La administración actual de la E.S.E HOSPITAL LOCAL se ha mejorado en un 95% su viabilidad económica, en la implementación de los nuevos cambios en los servicios de la salud, con la adquisición de nuevos equipos en las áreas de urgencias, sala de partos, terapia física, ginecología, y en los programas de promoción y prevención a través de los grupos extramurales, un cambio en la rama del personal asistencia con nuevos criterios.

Una visión con gestión, compromiso, y eficiencia se ha prestado en la administración actual, en el cual se ha mejorado la prestación del servicio de salud de la población, rural y urbana rió dórense, en el Pro de mejorar la calidad de vida con capacidad de gestión en recursos, tocando puertas en busca de nuevos horizontes en programa, proyectos y aunado esfuerzos para innovar el diario vivir y el cambio de la administración del área de salud.

4.1.1.5 Objeto Social. Prestación de servicios médicos de primer nivel de atención en:

Urgencias.
Consulta externa.
Odontología
Laboratorio clínico.
Promoción y prevención.
Terapias respiratorias y físicas.
Atención de enfermedades.

4.1.1.6 Objetivos.

Establecer el nivel de atención integral de salud, a la población que requiere los servicios de la E.S.E HOSPITAL LOCAL, a través de los servicios médicos, de la capacidad de gestión de la empresa.

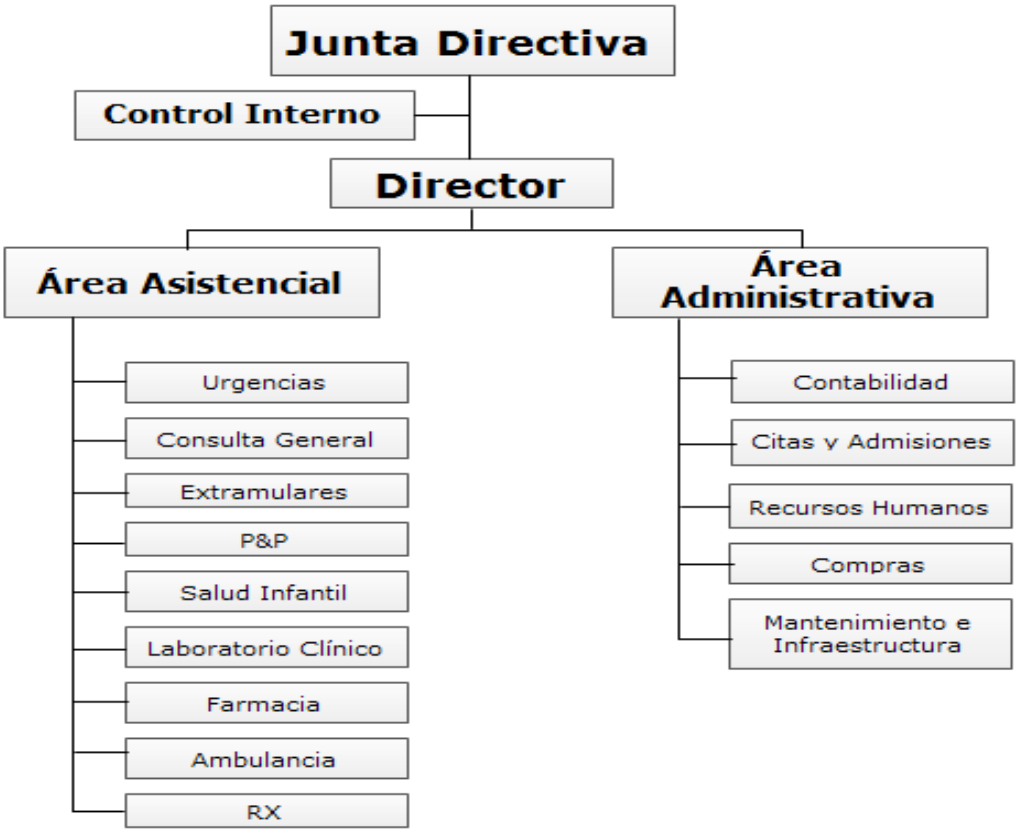
Evaluar las estrategias de atención, promoción y control en la prestación de los servicios de salud.

Asegurar el cumplimiento de la normatividad legal y administrativa en todos los niveles de la organización.

Garantizar la evaluación permanente y oportunidad de los aspectos fundamentales de la gestión adelantada por la E.S.E HOSPTITAL LOCAL.

Garantizar los niveles óptimos de eficiencia, eficacia y economía en todas las operaciones adelantadas por la E.S.E HOSPITAL LOCAL que está promoviendo.

4.1.1.7 Estructura Orgánica de la E.S.E Hospital Local de Rio de Oro Cesar.



4.2 MODELO DE NEGOCIOS PARA EL ÁREA DE CONTABILIDAD DE LA E.S.E HOSPITAL LOCAL DE RIO DE ORO CESAR.

El área contable de la ESE no tiene misión ni visión implementadas las cual proponemos la siguiente y evaluamos para medir su eficacia.

Misión propuesta: Área de Contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar. Cumplimos procesos organizados, dignos, oportunos y confiables el mejoramiento de la calidad de vida de los usuarios y la atención adecuada y a tiempo en cada uno de los servicios de la ESE desde el área financiera y contable ayudando a solucionar los problemas que se presenten y ser eficaces en la organización.

N°	CRITERIOS	PREGUNTA	SI	NO
1	Clientes	¿Quiénes son los clientes?	X	
2	Productos y servicios	¿cuáles son los servicios o productos más importantes'	X	
3	Mercados	¿Compite geográficamente?	X	
4	Tecnología	¿Cuál es la tecnología básica?	X	
5	Preocupación por supervivencia, crecimiento y rentabilidad	¿Cuál es la actitud de la organización en relación a metas económicas?	X	
6	Filosofía	¿Cuáles son las creencias básicas, los valores, las aspiraciones, las prioridades éticas de la organización?	X	
7	Concepto de si misma	¿Cuáles son las ventajas competitivas claves?	X	
8	Preocupación por la imagen pública	¿Cuál es la imagen pública a que aspira?, ¿Es responsable socialmente, ante la comunidad y el medio ambiente?	X	
9	Preocupación por los empleados	¿Son los empleados un valor activo para la organización? ¿Pone atención a los deseos de las personas claves, de los grupos de interés?	X	

Visión propuesta: Área de Contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar. Ser un área con ética, innovador y de una excelencia contable optima enfocada al servicio de la administración para el beneficio del sector salud del municipio de Rio de Oro conservando el reconocimiento a nivel departamental, regional y nacional.			
N°	**CRITERIO**	**SI**	**NO**
1	Orientado al futuro incluso en su redacción		X
2	Es integradora	X	
3	Es corta	X	
4	Es positiva y alentadora	X	
5	Es realista - posible	X	
6	Es consistente con los principios y valores de la organización	X	
7	Orienta la transición de los que es a lo que debe llegar a ser	X	
8	Expresa claramente los logros que se esperan en el periodo	X	
9	Cubre todas las áreas actuales y futuras de la organización	X	
10	Está redactada en términos que signifiquen acción	X	
11	Tienen fuerza e impulsa a la acción	X	
12	Contiene el futuro visualizado	X	
13	Es el sueño alcanzable a largo plazo	X	

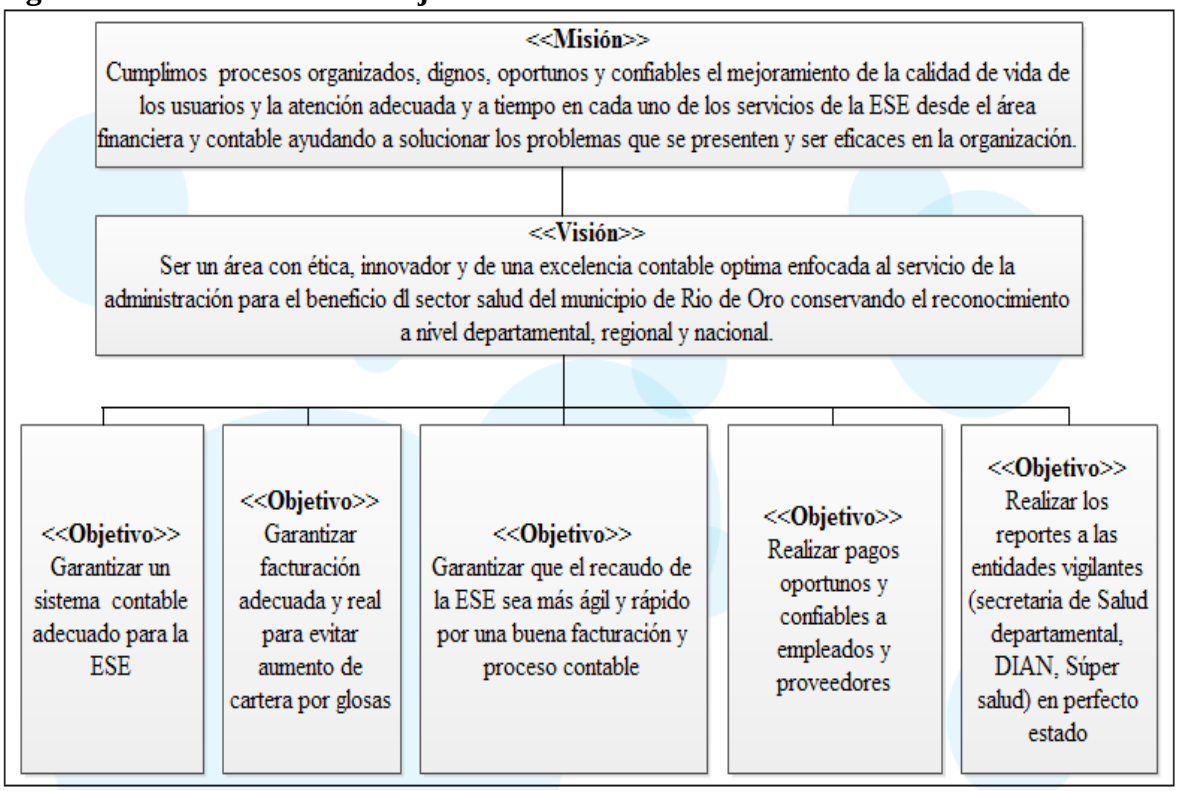
4.2.1 Misión. Cumplimos procesos organizados, dignos, oportunos y confiables el mejoramiento de la calidad de vida de los usuarios y la atención adecuada y a tiempo en cada uno de los servicios de la ESE desde el área financiera y contable ayudando a solucionar los problemas que se presenten y ser eficaces en la organización.

4.2.2 Visión. Ser un área con ética, innovador y de una excelencia contable optima enfocada al servicio de la administración para el beneficio dl sector salud del municipio de Rio de Oro conservando el reconocimiento a nivel departamental, regional y nacional.

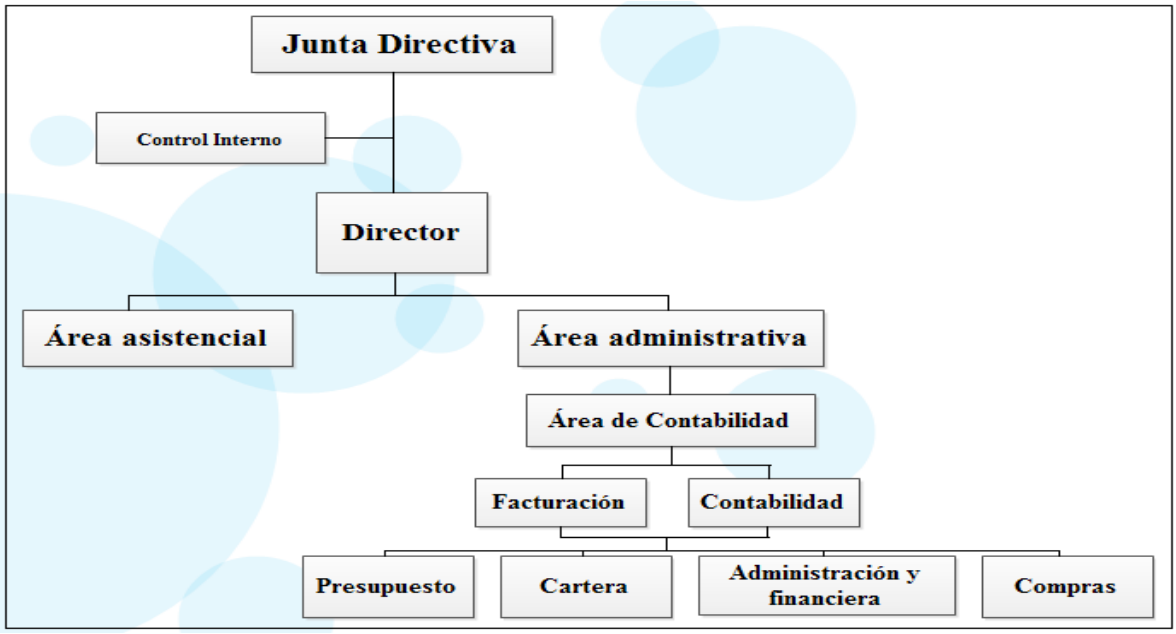
4.2.3 Objetivos.

- ✓ Garantizar un sistema contable adecuado para la ESE
- ✓ Garantizar facturación adecuada y real para evitar aumento de cartera por glosas
- ✓ Garantizar que el recaudo de la ESE sea más ágil y rápido por una buena facturación y proceso contable
- ✓ Realizar pagos oportunos y confiables a empleados y proveedores
- ✓ Realizar los reportes a las entidades vigilantes (secretaria de Salud departamental, DIAN, Súper salud) en perfecto estado

Figura 6. Misión – Visión – Objetivos



4.2.4 Estructura Orgánica del Área de Contabilidad.



4.3 MODELADO DE PROCESOS DEL NEGOCIO.

En el modelado de procesos del negocio del Área de Contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar se describen las actividades que permiten cumplir los objetivos específicos en la jerarquía de objetivos de negocio, las condiciones y reglas que deben cumplir y la definición de los responsables o roles de la ejecución del mismo.

4.3.1 Procesos Principales:

- **Área de contabilidad:**

Mantener el registro de los hechos contables en forma oportuna basada en el fiel apego a la realidad de la actividad económica del establecimiento, de acuerdo a la contabilidad del estado y a los requerimientos de gestión.

4.3.2 Procesos de Apoyo

- **Presupuesto:**

Determina los ingresos del hospital. Estos ingresos pueden venir de los pagos de los pacientes, dinero de los impuestos, donaciones o créditos de seguros. Asegúrate de deducir un porcentaje de las facturas de los pacientes que quedarán sin cobrar, el trabajo de caridad que se espera del hospital y el trabajo honorario que hace el hospital

Tienes que saber el costo del personal, de todos los empleados y el personal auxiliar, como los consultores, la contratación externa, y tal vez los servicios de personal de lavandería o enfermería. Calcula para todos los empleados del hospital (desde el personal de limpieza hasta los médicos), los beneficios sociales que el hospital debe pagarle a cada uno.

Para hacer el presupuesto, usa una hoja de cálculo. Introduce todas las categorías y el costo de cada una. Añade todos los ítems sujetos a impuestos y el porcentaje de cada uno. Es probable que obtengas tarifas reducidas en los servicios públicos, o por lo menos una reducción en los impuestos sobre ellos. Escribe todas las fórmulas para estos. Es posible que tu estado o el sistema de hospitales tengan una hoja de cálculo disponible. Si ya existe una, úsala o modifícala para que se ajuste a tus necesidades. Si no existe, haz una, para que hacer el presupuesto del próximo año sea simplemente introducir números y dejar que la computadora haga el resto del trabajo

- **Cartera:**

Planear: Se establecen objetivos, metas y planes a seguir para un buen recudo de la cartera

Organizar: Es el proceso mediante el cual los empleados y sus labores se unen para el cumplimiento de los objetivos, acidando un buen servicio al cliente y tratar de no dejar perder el crédito

Dirigir: A través de las políticas o lineamientos para que los créditos no sobresalgan sus límites C

Controlar: Se encarga de gestionar el cobro buscar la manera que los empleados no dejen perder la cartera y motivar a los clientes a sus oportunos pagos.

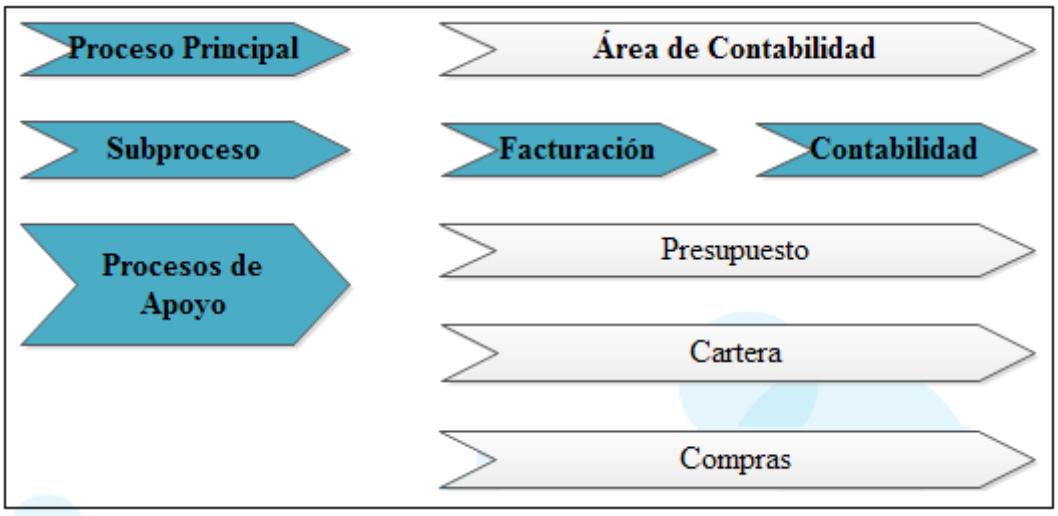
- **Compras:**

Se encarga de compra y los activos de la ESE durante el año y de acuerdo a las necesidades en la prestación del servicio

4.3.3 Diagrama de Actividades

El Área de Contabilidad ejecuta sus procesos utilizando la cadena de valor (ver figura).

Figura 7. Cadena de valor

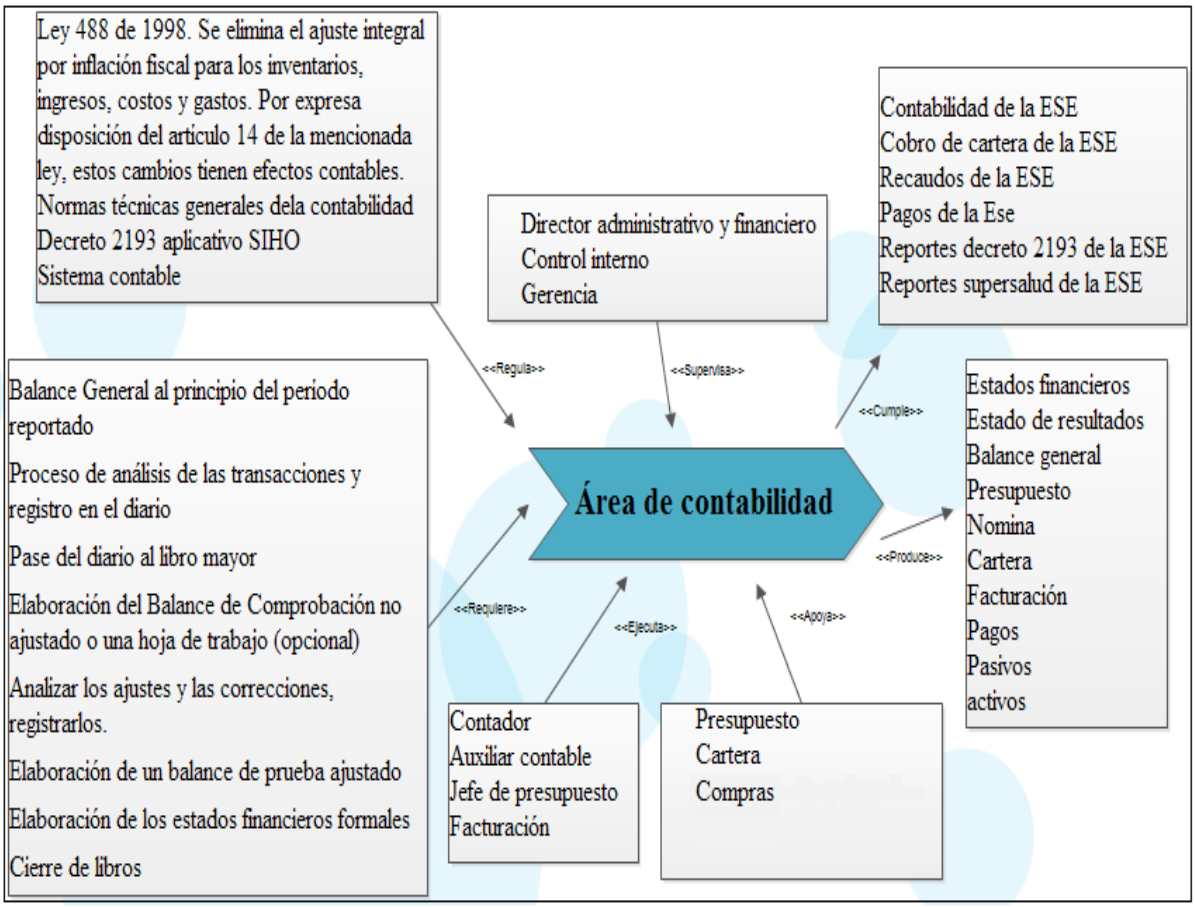


La descripción de cada uno de estos procesos se presenta en el diagrama de descripción de procesos de manera jerárquica.

Modelo de descripción de procesos

- **PF Área de Contabilidad:**

Mantener el registro de los hechos contables en forma oportuna basada en el fiel apego a la realidad de la actividad económica del establecimiento, de acuerdo a la contabilidad del estado y a los requerimientos de gestión.



La descripción de los subprocesos está compuesta por:

Figura 8. Subproceso del proceso Área de contabilidad

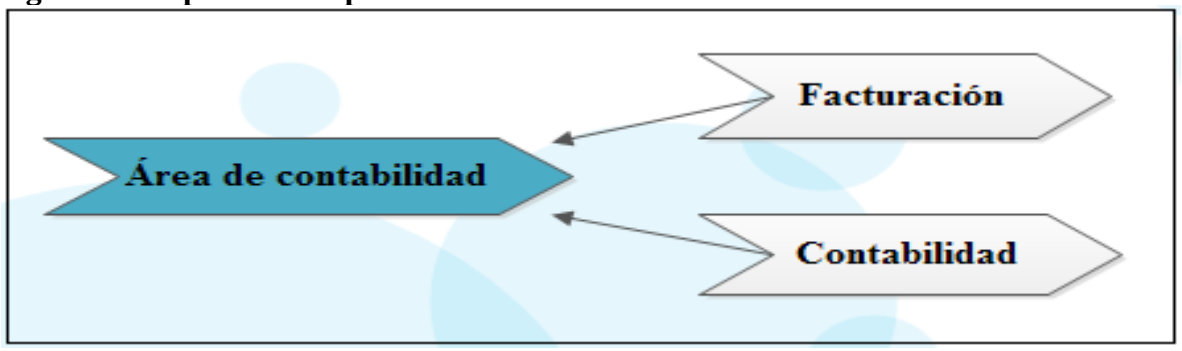


Figura 9. Subproceso Facturación

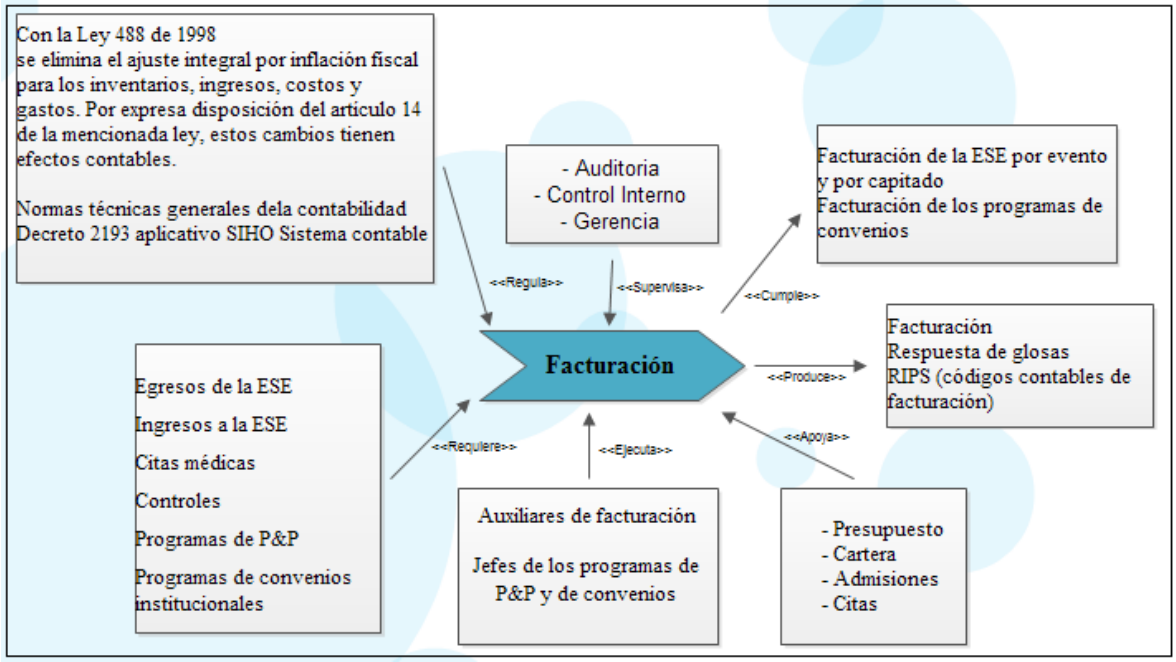
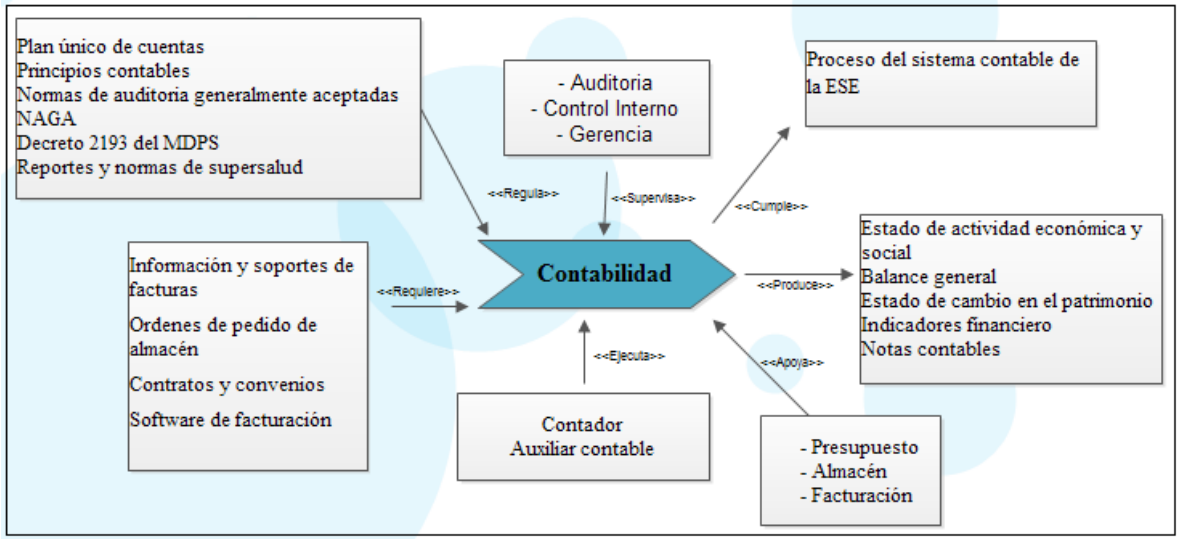


Figura 10. Subproceso Contabilidad



4.4 INFRAESTRUCTURA TECNOLÓGICA.

El Área de contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar, cuenta con equipos de cómputo en los espacios de trabajo. Se relacionan las características de los dispositivos para la ejecución de los procesos de la misma.

4.4.1 Dispositivos de cómputo e Impresora

Tabla 2. Equipos de cómputo del Área de Contabilidad y sus características.

Dispositivo	Características y/o especificaciones
PC Escritorio All in One (AIO) Contador	Hardware: -Procesador Intel® Xeon® 3GHz -RAM 2GB -Disco Duro 500 GB -Monitor de 20 pulgadas -Tarjeta de Red incorporada Software: -Sistema Operativo Windows XP Professional -Microsoft Office 2007 -Sistema Contable Integrado TNS
PC Escritorio All in One (AIO) Técnico administrativo contable	Hardware: -Procesador Intel® Xeon® 3GHz -RAM 2GB -Disco Duro 500 GB -Monitor de 20 pulgadas -Tarjeta de Red incorporada Software: -Sistema Operativo Windows XP Professional -Microsoft Office 2007 -Sistema Contable Integrado TNS
PC Escritorio HP All in One (AIO) Presupuesto	Hardware: -Procesador Intel® Xeon® 3GHz -RAM 2GB -Disco Duro 500 GB -Monitor de 20 pulgadas -Tarjeta de Red incorporada Software: -Sistema Operativo Windows XP Professional -Microsoft Office 2007 -Sistema Contable Integrado TNS
Impresora Láser	Marca Xerox Ref. 3600 DN Color blanco y negro hasta 38 PPM

4.4.2 Proveedor de Servicios de Internet ASTECA. Azteca Comunicaciones Colombia es una empresa del Grupo Salinas de México, que tiene la responsabilidad de implementar el Proyecto Nacional de Fibra Óptica del Programa Compartel, que hace parte del Ministerio de las Tecnologías de la Información y las Telecomunicaciones.

4.4.3 Tipo de red. El Área de contabilidad se encuentra inmersa en la red LAN de la E.S.E Hospital Local de Rio de Oro Cesar, conectada con cable UTP categoría 5e.

4.4.4 Topología. La topología usada en la E.S.E Hospital Local de Rio de Oro Cesar es estrella.

El área de contabilidad se interconecta con las siguientes oficinas:

- Farmacia / almacén
- Facturación / urgencias
- Facturación / consulta externa
- Presupuesto
- Tesorería

4.4.5 Sistema Operativo.

Los sistemas operativos de los equipos de cómputo del Área de Contabilidad son Windows XP Professional.

4.4.6 Sistemas de Información

TNS SAS

NIT.800.182.856-1

Sistema contable integrado visual TNS sector oficial, Módulos: Modulo contabilidad, Tesorería, Presupuesto, Almacén, Activos fijos, Facturación hospitalaria y cartera.

Especificaciones mínimas de los equipos

-Procesador Intel® Xeon® 3GHz
-2GB de memoria RAM
-Espacio libre de Disco Duro de 500MB
-Windows XP Professional, preferiblemente Windows Server
-UPS Para protección

Terminal

-Procesador Pentium IV de 1.5 GHz

-1 GB de Memoria RAM
-Espacio libre Disco Duro de 200MB
-Tarjeta de Red (No genérica)
-Windows XP o superior

Nota: La red debe ser cableada NO se recomienda redes inalámbricas.

4.5 ANÁLISIS Y TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL ÁREA DE CONTABILIDAD DE LA E.S.E.

4.5.1 Análisis y tratamiento de riesgos

Para proceder a realizar el análisis y el tratamiento de riesgos, debemos definir el alcance del SGSI. Luego de haber definido el alcance del sistema, tras haber identificado los procesos del área de contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar, se procede a analizar el flujo de cada uno de los procesos, de una manera más detallada, y se identifican las vulnerabilidades que se pueden encontrar dentro del flujo de los procesos.

Tabla 3. Niveles de Riesgo

Matriz de Análisis de Riesgos 5x5					
	5x5 Impacto				
Probabilidad de Ocurrencia	**Muy Bajo**	**Bajo**	**Medio**	**Alto**	**Muy Alto**
Muy Alto			Perdida o daño de capacidades operativas a causa de problemas con el sistema de información del área contable de la ESE	No reclutar, desarrollar o retener a los empleados que cuenten con habilidades o conocimientos Apropiados.	Desconocimiento del software que se aplica en contabilidad y desactualización de los módulos del mismo No implementación de un sistema que garantice la tecnología de la información en el área contable en la ESE
Alto			Perdida de la información Pérdida de clientes	Pérdida o daño de capacidades operativas a causa de problemas con los equipos	

			Mala selección del personal que labora en el área contable de la ESE No cumplimiento con el presupuesto planteado para las vigencias anuales Servicio inoportuno y demorado a los clientes.	Perdida de disponibilidad de información Fallas de sistemas de información. Uso inapropiado de información	
Medio		Incapacidad de planear y gestionar los recursos requeridos para un proyecto Riesgo de selección adversa Efecto negativo de la opinión pública desde el punto de vista contable Calidad deficiente de los servicios proporcionados por proveedores externos .	negocio Incapacidad de planear, gestionar y monitorear el desempeño de proyectos, productos, servicios, procesos, personal y canales de información relacionados con Tecnología. Mal manejo de presupuesto publico Incumplimiento de las metas en el plan de gestión del gerente de la ESE Uso inapropiado de información	No evaluar adecuadamente las capacidades de los proveedores pérdidas financieras difícil cobro de carteta de la ESE mayor a 360 días	
Bajo			Pérdida o daño de capacidades		

			operativas a causa de problemas con las instalaciones		
Muy Bajo			Pérdida o daño de información u objetos de valor a causa de fraude, robo, negligencia voluntaria, negligencia grave,		Pérdida parcial o total de la información a causa de un desastre natural

Tabla 4. Matriz de tratamiento de riesgos

PROCESO	ÁREA DE CONTABILIDAD																
1. IDENTIFICACIÓN DEL RIESGO				2. VALORACION	3. ANALISIS										4. EVALUACION		
Actividad	Riesgo	Factor de riesgo (Interno - Externo) Causas	Consecuencias	Controles	PROBABILIDAD					IMPACTO NEGATIVO					CALIFICACION DEL RIESGO		
					Improbable	Remoto	Factible	Probable	Muy probable	Insignificante	Bajo	Medio	Grave	Muy Grave	Alto	Moderado	Bajo	Insignificante
					1	2	3	4	5	1	2	3	4	5	NIVEL DE RIESGO		
Procesos de área contable de la ESE	Perdida o daño de capacidades operativas a causa de problemas con el sistema de información del área contable de la ESE	No implementación de un sistema de información a tiempo Desorden en el área contable	• Perdida de información por desactualización del software • Perdida de información por desconocimiento del proceso • Información entregada en informes errónea e incompleta	• Desarrollar políticas sobre adquisición y desarrollo del software dentro del área contable de la ESE • Realizar un proceso de certificación adecuado antes de realizar informes y trasladas información ya sea a procesos internos o externos • Realizar programas de capacitación enfocados a los sistemas de información utilizados				x					x		15		

				dentro del área contable de la ESE											
Procesos de área contable de la ESE	Desconocimiento del software que se aplica en contabilidad y desactualización de los módulos del mismo	La no compra del software de área contable ni la actualización del mismo	• Perdida de información importante del área contable • Demora en el proceso contable • Registros no reales de la parte financiera de la ESE • Malos registros e información inadecuada en el sistema contable de la ESE	• Ejecutar el contrato de actualización del sistema contable de la ESE • Capacitación al personal del software del sistema contable de la ESE				**x**					**x**		**25**
Proceso de área contable de la ESE	No implementación de un sistema que garantice la tecnología de la información en el área contable en	Falta de implementación de los procesos de la ESE	• Desorden en el sistema de información de la ESE • Perdida de información • Desorden administrativa y financieramente en el área contable de la ESE	• Implementar un sistema de que garantice el sistema de información contable el la ESE				**x**					**x**		**25**
Proceso de Recursos Humanos de la ESE	No reclutar, desarrollar o retener a los empleados que cuenten con habilidades o conocimientos Apropiados.	No implementación del proceso de recursos humanos de la ESE	• Mal manejo del sistema de información • Errores en el suministro de la	• Imprentar un proceso de reclutamiento del personal para el área contable adecuado que				**x**				**x**			**16**

			información contable de la ESE • Desorden en el área contable • No confiabilidad en la información suministrada para el área contable	incorpore perfiles de los cargos de acuerdo a las competencias requeridas para tal labor											
Departamento de sistemas de la ESE	Pérdida o daño de capacidades operativas a causa de problemas con los equipos	Equipos obsoletos y falta de mantenimiento preventivo y correctivo a los equipos de la ESE	• Perdida de información importante del área contable	• Realizar proyectos que garanticen la compra d nuevos equipos • Realizar programa de mantenimiento correctivo y preventivo y cumplirlos en los tiempos adecuados				**x**				**x**			**16**
Area contable de la ESE	Perdida de disponibilidad de información	Debido a la desactualización del sistema y falta de comunicación entre las áreas almacén – contabilidad – presupuesto	• Falta de confiabilidad en la información contable • Registros contables no reales e incompletos • Errores en los estados financieros y estados de resultados en la Ese • Cuellos de botella al	• Creación de un sistema de seguridad de la información en el área contable para evitar las perdidas				**x**				**x**			**16**

			interactuar con otros procesos de la organización												
Área Contable	Uso inapropiado de información	Debido a la falta de implementación de proceso en la ESE	• Perdida de información. • Falta de confiabilidad en el proceso contable • Informes mal reportados a los entes de control • Fuga de información a la competencia	• Implementar un sistemas de tecnología de la información que garantice el uso apropiado de la información generada por el ara contable de la ESE así como la de sus clientes internos y externos • Capacitación al personal del área contable y subprocesos que lo apoyan sobre el uso apropiado de la información de la ESE			**x**			**x**					**16**

Figura11. Criterios de análisis y evaluación de riesgos

ANALISIS

IMPACTO / CONSECUENCIA	CUANTIFICACIÓN	DESCRIPCIÓN
Insignificante	1	· No hay daños o perjuicios.
		· La pérdida financiera es baja.
		· No hay pérdida de imagen.
Bajo	2	· Se puede subsanar los daños inmediatamente.
		· La pérdida financiera es media.
		· No hay pérdida de imagen.
Medio	3	· Se necesita asistencia de un tercero para subsanar los daños.
		· La pérdida financiera es alta.
		· Podría existir pérdida de imagen.
Grave	4	· Daños extensivos, pérdida de la capacidad de operación que no tiene efectos perjudiciales.
		· Pérdidas financieras mayores.
		· Pérdida de imagen
Muy grave	5	· Pérdida de la capacidad de operación que tiene efectos perjudiciales.
		· Enorme pérdida financiera.
		· Grave pérdida de imagen.

EVALUACION

IMPACTO / PROBABILIDAD		Insignificante	Bajo	Medio	Grave	Muy Grave
PROBABILIDAD		1	2	3	4	5
Muy probable	5	5	10	15	20	25
Probable	4	4	8	12	16	20
Factible	3	3	6	9	12	15
Remoto	2	2	4	6	8	10
Improbable	1	1	2	3	4	5

Nota: no se tendrán en cuenta la evaluacion como insignifioante, se tomara como bajo

Riesgo Insignificante		
Riesgo Bajo		Gestionar mediante procedimientos de rutina, es improbable que se necesite la aplicación específica de recursos
Riesgo Moderado		Gestionar mediante procedimientos de monitoreo o respuesta específicas.
Riesgo Alto		Acción inmediata, especificar planes de acción y atención de la alta dirección.

PROBABILIDAD	CUANTIFICACIÓN	DESCRIPCIÓN	FRECUENCIA
Improbable	1	El evento ocurriría solamente en circunstancias excepcionales.	No se ha presentado en los últimos 5 años
Remoto	2	El evento podría ocurrir en algún momento y se considera que es difícil que suceda.	Al menos 1 vez en los últimos 5 años
Factible	3	El evento puede suceder eventualmente.	Al menos 1 vez en los últimos 2 años
Probable	4	El evento probablemente ocurrirá.	Al menos 1 vez en el último año
Muy probable	5	Se espera que el evento ocurra en la mayoría de los casos.	Más de 1 vez al año.

IMPACTO DE LA CONSECUENCIA POSITIVA	CUANTIFICACION	DESCRIPCION
Insignificante	1	Ganancias financieras pequeñas.
Menor	2	Ganancia financiera media.
Moderada	3	Ganancia financiera alta.
Importante	4	Ganancias financieras considerables.
Mayor	5	Ganancia financiera enorme.

4.6 DIAGNOSTICO DE LA INFORMACIÓN DEL ÁREA DE CONTABILIDAD DE LA E.S.E HOSPITAL LOCAL DE RIO DE ORO CESAR.

Para la realización del diagnóstico de la seguridad de la información del Área de contabilidad, se realizó una Auditoria administrativa y de Sistemas de Información (Ver Anexo**),** la cual tenía como objetivo Evaluar el funcionamiento administrativo, evaluar la seguridad en la protección y conservación de locales, instalaciones, mobiliario, equipos y evaluar la seguridad en la información y bases de datos del área de contabilidad de la ESE Hospital Local de Rio de Oro Cesar. Las herramientas de recolección de datos utilizada fueron: revisión documental, observación directa, entrevistas informal y aplicación de encuestas.

4.7 IDENTIFICACIÓN DE LOS ELEMENTOS QUE CONFORMAN EL SGSI – SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE CONTABILIDAD DE LA E.S.E

Se realizara una comparación entre las normas ISO/IEC 27002, ISO/IEC 27001 y COBIT 4.1, para determinar cuál de estas se tomara como base para el desarrollo del Sistema de Gestión de Seguridad de la Información SGSI y la Política de Seguridad de la Información.

4.8 COMPARATIVA ENTRE ISO/IEC 27002, ISO/IEC 27001 Y COBIT 4.1

Actualmente existen varios estándares certificables que garantizan la protección de los Sistemas Informáticos así como un buen uso de la información. Poseer alguno de estos estándares significa cumplir con la Ley Orgánica de Protección de Datos (LOPD) ya que impone controles más restrictivos que esta ley.

El principal estándar de seguridad informática y de la información, que define los requisitos de auditoría y sistemas de gestión de seguridad de la información es el ISO/IEC 27001. Este estándar puede usarse en conjunción con el ISO/IEC 27002, el cual se conforma como un código internacional de buenas prácticas de seguridad informática y de la información.
Existen otros estándares de carácter más general que también cubren la seguridad informática como parte del desarrollo de una infraestructura de tecnología de la información completa. Ejemplos de este tipo son COBIT (Objetivos de Control de la Tecnologías de la Información). Estos estándares surgen como buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información.

4.8.1 ISO/IEC 27002[20]

El ISO/IEC 27002, también conocido como ISO 17799, es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigida a los responsables de iniciar, implantar o mantener la seguridad de una organización.

El objetivo de la norma ISO/IEC 27002 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

Se trata de una norma no certificable, pero que recoge la relación de controles a aplicar para establecer un SGSI.

Estructura del estándar:

El ISO/IEC 27002 contiene 11 cláusulas de control de seguridad conteniendo colectivamente un total de 39 categorías de seguridad principales.

A continuación se detallan las diferentes cláusulas con sus categorías y los objetivos que persiguen cada una de ellas:

1. Política de Seguridad

- **Política de seguridad de la información.** Proporcionar a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes.

2. Organización de la Seguridad de la Información

- **Organización interna.** Manejar la seguridad de la información dentro de la organización.
- **Grupos o personas externas.** Mantener la seguridad de la información y los medios de procesamiento de información de la organización que son ingresados, procesados, comunicados o manejados por, grupos externos.

3. Gestión de Activos

- **Responsabilidad por los activos.** Lograr y mantener una apropiada protección de los activos organizacionales.
- **Clasificación de la información.** Asegurar que la información reciba un nivel de protección apropiado.

[20] JIMENEZ RUIZ, Alberto. myEchelon: Un sistema de Auditoría de Seguridad Informática Avanzado bajo GNU/Linux. Universidad de Almería. Almería, España. 217 h. [en línea]. http://www.adminso.es/images/9/9c/Alberto_PFC.pdf.

4. Seguridad de Recursos Humanos

- **Antes del empleo.** Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados, y reducir el riesgo de robo, fraude y mal uso de los medios.
- **Durante el empleo.** Asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.
- **Finalización o cambio de empleo.** Asegurar que los usuarios empleados, contratistas y terceras personas salgan de la organización o cambien de empleo de una manera ordenada.

5. Seguridad Física y Ambiental

- **Áreas seguras.** Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.
- **Equipo de seguridad.** Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.

6. Gestión de Comunicaciones y Operaciones

- **Procedimientos y responsabilidades operacionales.** Asegurar la operación correcta y segura de los medios de procesamiento de la información.
- **Gestión de la entrega del servicio de terceros.** Implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros.
- **Planificación y aceptación del sistema.** Minimizar el riesgo de fallos en el sistema.
- **Protección contra el código malicioso y móvil.** Proteger la integridad del software y la integración.
- **Copia de Seguridad.** Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.
- **Gestión de seguridad de la red.** Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.
- **Gestión de medios.** Evitar la divulgación no-autorizada, la modificación, eliminación o destrucción de activos y la interrupción de las actividades comerciales.
- **Intercambio de información.** Mantener la seguridad en el intercambio de información y software dentro de la organización y con cualquier otra entidad externa.
- **Servicios de comercio electrónico.** Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro.
- **Monitorización.** Detectar las actividades de procesamiento de información no autorizadas.

7. Control de Acceso

- **Requerimiento del negocio para el control del acceso.** Controlar el acceso a la información.
- **Gestión de acceso del usuario.** Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.
- **Responsabilidades del usuario.** Evitar el acceso de usuarios no-autorizados, evitar poner en peligro la información y evitar el robo de información y los medios de procesamiento de la información.
- **Control de acceso a la red.** Evitar el acceso no autorizado a los servicios de la red.
- **Control del acceso al sistema operativo.** Evitar el acceso no autorizado a los sistemas operativos.
- **Control de acceso a la aplicación y la información.** Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.
- **Computación y tele-trabajo móvil.** Asegurar la seguridad de la información cuando se utiliza medios de computación y tele-trabajo móvil.

8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

- **Requerimientos de seguridad de los sistemas de información.** Garantizar que la seguridad sea una parte integral de los sistemas de información.
- **Procesamiento correcto en las aplicaciones.** Prevenir errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones.
- **Controles criptográficos.** Proteger la confidencialidad, autenticidad o integridad a través de medios criptográficos.
- **Seguridad de los archivos del sistema.** Garantizar la seguridad de los archivos del sistema.
- **Seguridad en los procesos de desarrollo y soporte.** Mantener la seguridad del software y la información del sistema de aplicación.
- **Gestión de la Vulnerabilidad Técnica.** Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

9. Gestión de Incidentes de Seguridad de la Información

- **Informe de los eventos y debilidades de la seguridad de la información.** Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.
- **Gestión de los incidentes y mejoras en la seguridad de la información.** Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información.

10. Gestión de la Continuidad Comercial

- **Aspectos de la seguridad de la información de la gestión de la continuidad del negocio.** Contraatacar las interrupciones a las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallos importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

11. Cumplimiento

- **Cumplimiento de los requerimientos legales.** Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.

- **Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico.** Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.

- **Consideraciones de auditoría de los sistemas de información.** Maximizar la efectividad de y minimizar la interferencia desde/hacia el proceso de auditoría del sistema de información.

4.8.2 ISO/IEC 27001[21]

Este estándar internacional ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización.

En función del tamaño y necesidades se implementa un SGSI con medidas de seguridad más o menos estrictas, que en cualquier caso pueden variar a lo largo del tiempo.

Enfoque del proceso

Una organización necesita identificar y manejar muchas actividades para poder funcionar de manera efectiva. Cualquier actividad que usa recursos y es manejada para permitir la transformación de éstos en outputs, se puede considerar un proceso.

[21] JIMENEZ RUIZ, Alberto. myEchelon: Un sistema de Auditoría de Seguridad Informática Avanzado bajo GNU/Linux. Universidad de Almería. Almería, España. 217 h. [en línea]. http://www.adminso.es/images/9/9c/Alberto_PFC.pdf.

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación y las interacciones de estos procesos, y su gestión, puede considerarse un enfoque del proceso.

El enfoque del proceso para la gestión de la seguridad de la información que presenta este estándar internacional fomenta que sus usuarios enfaticen la importancia de:

- Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
- Implementar y operar controles para manejar los riesgos de la seguridad de la información.
- Monitorizar y revisar el desempeño y la efectividad del SGSI.
- Mejora continua en base a la medición del objetivo.

Este estándar Internacional adopta el modelo del proceso Planificar-Hacer-Comprobar-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI.

La figura muestra como un SGSI toma como entrada los requerimientos y expectativas de la seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que satisfacer aquellos requerimientos y expectativas.

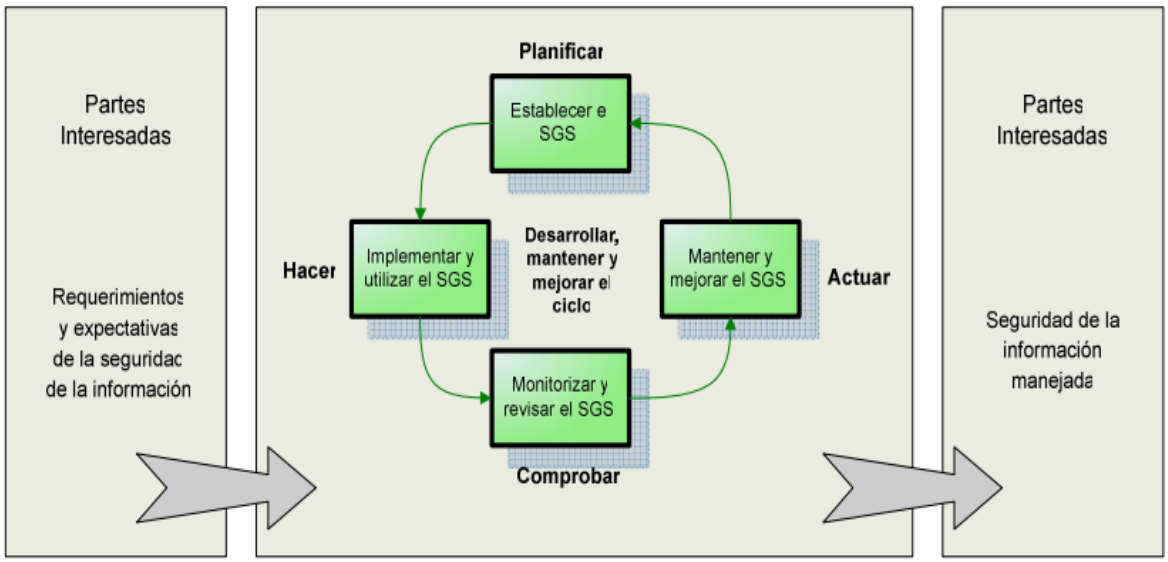


Figura 12. Modelo PDCA aplicado a los procesos SGSI

La siguiente tabla muestra en profundidad una descripción de las acciones llevadas a cabo en cada uno de los estados del modelo PDCA.

Tabla 5. Acciones realizadas en el modelo PDCA.

Estado	Acciones
Planificar (establecer el SGSI)	Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.
(Implementar y utilizar el SGSI)	Implementar y utilizar la política, controles, procesos y procedimientos SGSI.
Comprobar (Monitorizar y revisar el SGSI)	Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias practicas del SGSI e informar de los resultados a la gerencia para su revisión.
Actuar (Mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr la mejora continua del SGSI.

Compatibilidad con otros sistemas de gestión

Este estándar internacional es compatible con el ISO 9001:2000 e ISO 14001:2004 para dar soporte a una implementación y operación consistente e integrada con los estándares de gestión relacionados. Por lo tanto, un sistema de gestión adecuadamente diseñado puede satisfacer los requerimientos de todos estos estándares.

Además se puede utilizar en conjunción con el estándar ISO/IEC 27002 que proporciona un modelo contrastado para la implementación de los controles de seguridad.

4.8.3 COBIT 4.1[22]

COBIT (Control Objectives for Information and related Technology) es el marco aceptado internacionalmente para el control de la información.

COBIT determina, con el respaldo de las principales normas técnicas internacionales, un conjunto de mejores prácticas para la seguridad, la calidad, la eficacia y la eficiencia en Tecnologías de la Información TI, que son necesarias para alinear TI con el negocio,

[22] JIMENEZ RUIZ, Alberto. myEchelon: Un sistema de Auditoría de Seguridad Informática Avanzado bajo GNU/Linux. Universidad de Almería. Almería, España. 217 h. [en línea]. http://www.adminso.es/images/9/9c/Alberto_PFC.pdf.

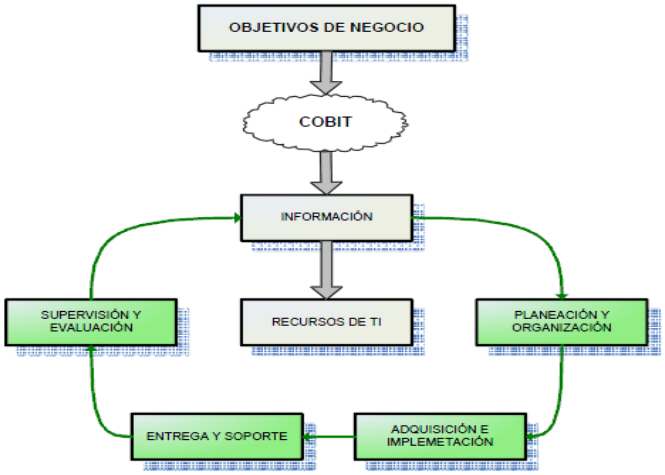
identificar riesgos, entregar valor al negocio, gestionar recursos y medir el desempeño, el cumplimiento de metas y el nivel de madurez de los procesos de la organización.

COBIT fue creado por la Information Systems Audit and Control Association (ISACA) y el IT Governance Institute (ITGI) en 1992.

Actualmente, se ha publicado la versión de COBIT 4.1 que tiene 34 objetivos de alto nivel que cubren 318 objetivos de control clasificados en cuatro dominios: Planificación y Organización, Adquisición e Implementación, Entrega y Soporte, y Supervisión y Evaluación.

La figura 19 muestra la relación existente entre los diferentes dominios que forman el estándar COBIT:

Figura 13. Dominios de COBIT 4.1



Fuente: JIMENEZ RUIZ, Alberto.

A continuación se muestran las funciones desempeñadas por cada uno de los dominios mostrados en la figura 19:

Planificación y Organización

- Definir un plan estratégico de TI.
- Definir la arquitectura de la información.
- Determinar la dirección tecnológica.
- Definir la organización de las relaciones de TI.
- Manejar la inversión en TI.
- Comunicar la Dirección y aspiraciones de la Gerencia.
- Administrar Recursos Humanos.
- Asegurar el cumplimiento de requisitos externos.
- Evaluar riesgos.

- Administrar proyectos.
- Administrar calidad.

Adquisición e Implementación

- Identificar soluciones.
- Adquirir y mantener software de aplicación.
- Adquirir y mantener arquitectura de la tecnología.
- Desarrollar y mantener procedimientos relacionados con TI.
- Instalar y acreditar sistemas.
- Administrar cambios.

Entrega y Soporte

- Definir y manejar niveles de servicio.
- Administrar servicios prestados por terceros.
- Administrar Desempeño y Capacidad.
- Asegurar servicio continuo.
- Garantizar la Seguridad de Sistemas.
- Identificar y asignar costos.
- Educar y entrenar a los usuarios.
- Apoyar y asistir a los clientes de TI.
- Administrar la configuración.
- Administrar problemas e incidencias.
- Administrar Datos.
- Administrar Instalaciones.
- Administrar Operaciones.

Supervisión y Evaluación

- Supervisar los procesos.
- Evaluar lo adecuado del control interno.
- Obtener aseguramiento independiente.
- Proporcionar auditoría independiente.

4.8.4 Factores de comparación.

NORMA FACTORES	ISO/IEC 27001	COBIT 4.1	ISO/IEC 27002
Descripción	Es un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la Seguridad de la información (SGSI). Esta norma se puede usar para evaluar la conformidad, por las partes interesadas, tanto Internas como externas.	COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas). Es un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización.	Es una guía que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.
Estructura	PHVA Planear – Hacer – Verificar – Actuar.	Está definida por 34 objetivos de alto nivel que cubren 318 objetivos de control clasificados en cuatro dominios.	Está compuesta por once dominios, 39 objetivos de control y 133 controles para seguridad de la información.
Carácter con el cual es sustentado	Marco de Mejores Prácticas.	Marco de Mejores Prácticas.	Marco de Mejores Prácticas. Es un anexo del Estándar 27001 para la seguridad de la información.
Objetivo	Especificar los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI Documentado dentro del contexto de los riesgos globales del negocio de la organización. Especifica los requisitos para la implementación de controles de seguridad adaptados a las Necesidades de las	Investigar, desarrollar, publicitar y promocionar un marco de trabajo de control de gobierno de TI autoritativo, actualizado, y aceptado internacionalmente que se adopte por las empresas.	Este estándar internacional establece las guías y principios generarles para iniciar, implementar, mantener, y mejorar la gestión de seguridad de la información en una organización. Sus objetivos de control y controles son recomendados para cubrir los requerimientos de seguridad que han salido de una evaluación de riesgos.

	organizaciones individuales o a partes de ellas.		
Metas	- Asegurar controles de seguridad suficiente y proporcional que protejan los activos de información y brinden confianza a las partes interesadas. -Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización. -Implementar y operar la política, los controles, procesos y procedimientos del SGSI. -Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión. -Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.	-Enfocarse en objetivos y necesidades del negocio mejorando la cooperación y comunicación entre los administradores del negocio y los auditores. -Ayuda a los administradores a entender como los asuntos de seguridad y control benefician sus áreas de operación. -Ayudan a las organizaciones a compararse con la competencia e implementar mejores prácticas de objetivos de control y la tecnología relacionada. -Se desarrollan fuertes relaciones de negocio a varios niveles y las sorpresas se vuelven raras. -Las organizaciones generan confianza y credibilidad hacia sus clientes. -Permite a las organizaciones cumplir con requerimientos regulatorios. -Calidad de requerimientos de negocio y para el desarrollo de métricas que permitan la medición con respecto a estas metas.	Brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI), influenciado por las necesidades y objetivos, los procesos empleados y el tamaño y estructura de la organización.

Utilización	Esta norma está alineada con la NTC-ISO 9001:2000 y la NTC-ISO 14001:2004, con el fin de apoyar la implementación y operación, consistentes e integradas con sistemas de gestión relacionados.	Es una herramienta de clase mundial por excelencia implementada por las grandes organizaciones para adecuar sus sistemas de información a las mejores prácticas en materia de control y gobierno de TI.	Provee de herramientas a administradores de sistemas de gestión, alta dirección y auditores para ejecutar su labor e identificar sinergias que permitan una implementación/evaluación costo-eficiencia para la compañía.
Orientado	Sistemas de seguridad de la información.	Negocio.	Seguridad de la información.
A quien está dirigida	Esta norma está diseñada para las organizaciones independientemente de su tipo, tamaño y naturaleza.	El marco de control de COBIT a Auditores, Administradores, personal del negocio, Consultores, Ingenieros y en general a todos los niveles de una organización donde se requiera implantar un Gobierno de TI utilizando el marco de COBIT.	Cualquier persona en la organización que procese información. Es apropiado para pequeños negocios independientes, para los que es necesario tener un conocimiento básico sobre la seguridad de la información. También puede ser un buen comienzo para nuevos profesionales de la seguridad de la información.
Herramientas que se Utilizan	-Aceptación del riesgo. -Activos de la Organización -Análisis del Riesgo -Confidencialidad -Declaración de aplicabilidad -Evaluación de Riesgos -Seguridad de la Información	-Resumen ejecutivo -Marco referencial -Objetivos de control -Guías de auditoria -Conjunto de herramientas de implementación. -Guías gerenciales	-Intercambio y movilidad (Red externa y red local). -Soportes físicos. -Servicios externos. -Seguridad física. -Desarrollo y Mantenimiento (Documentación, servidores, aplicaciones y puestos de trabajo). -Organización. -Usuarios.
Confiabilidad	Alta	Alta	Alta
Enfoque Manejado	Operacional	Táctico	Táctico
Desventaja	Claridad en los planes de continuidad del negocio. Mantener una sola estructura de los planes	No incluye los pasos del proceso y las tareas ya que, si bien se orienta hacia los procesos de TI, es un marco de gestión y control en lugar de un	-Requiere esfuerzo continuo, al iniciar este conjunto de tareas, no cabe duda que se está sobrecargando el ritmo habitual de trabajo de toda

	de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento. Se pueden generar acciones de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales).	marco de proceso. Asimismo, COBIT se centra en lo que la empresa tiene que hacer, no cómo debe hacerlo y el público objetivo es la alta dirección, alta dirección de TI y los auditores. Con el incremento de las tecnologías de punta y la necesaria generalización de las aplicaciones informáticas de auditoría, el auditor tradicional debe enfrentarse al cambio, por lo que tendrá que vencer los retos que este cambio representa; entre ellos pueden señalarse los siguientes: Nueva Técnica Informática, su Auditabilidad e impacto en los procedimientos y controles, adaptar conceptos clásicos de control a la nueva tecnología, desarrollo de nuevas técnicas y herramientas para obtener evidencias.	la organización, por lo tanto se debe ser consciente de que exigirá un esfuerzo adicional. -Cuando el mejoramiento se concentra en un área específica de la organización, se pierde la perspectiva de la interdependencia que existe entre todos los miembros de la empresa. -Requiere de un cambio en toda la organización, ya que para obtener el éxito es necesaria la participación de todos los integrantes de la misma y a todo nivel. -En vista de que los gerentes en la pequeña y mediana empresa son muy conservadores, el mejoramiento continuo se hace un proceso muy largo. -Hay que hacer inversiones importantes.
Ventajas	Formula un plan para el tratamiento de riesgos que identifican la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información. Implementa el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que incluye considerar la	Se puede utilizar al más alto nivel, proporcionando un marco de control general sobre la base de un modelo de procesos de TI que debe adaptarse a cada organización de forma genérica. COBIT proporciona respuesta a las necesidades de la empresa, está orientado al negocio y diseñado para ser utilizado no solo por proveedores de servicios, usuarios y auditores de	En lo legislativo. -Protección de data y privacidad de la información personal -Protección de los registros organizacionales -Derechos de propiedad intelectual Los controles considerados práctica común para la seguridad de la información incluyen: -Documento de la política de seguridad de la información -Asignación de responsabilidades de la

	financiación y la asignación de funciones y responsabilidades. Define cómo medir la eficacia de los controles o grupos de controles seleccionados, y especificar cómo se van a usar estas mediciones con el fin de valorar la eficacia de los controles para producir resultados comparables y reproducibles. Gestiona la operación del SGSI. Implementa procedimientos y otros controles para detectar y dar respuesta oportuna a los incidentes de seguridad. Realiza revisiones regulares de la eficacia del SGSI (que incluyen el cumplimiento de la política y objetivos del SGSI, y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorias de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.	TI, sino también como guía integral para la gerencia y los mismos propietarios de la empresa. El marco de trabajo COBIT ofrece herramientas para garantizar la alineación con los requerimientos del negocio. Contribuye a estas necesidades de la siguiente manera: -Estableciendo un vinculo con los requerimientos del negocio. -Organizando las actividades de TI en un modelo de procesos generalmente aceptado. -Identificando los principales recursos de TI a ser utilizados. -Definiendo los objetivos de control gerenciales a ser considerados.	seguridad de la información -Conocimiento, educación y capacitación en seguridad de la información -Procesamiento correcto en las aplicaciones -Gestión de la vulnerabilidad técnica -Gestión de la continuidad comercial -Gestión de los incidentes y mejoras de la seguridad de la información. -La ISO 27001 y 27002 establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos delineados en este Estándar Internacional proporcionan un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados. -Sirve como un lineamiento práctico para desarrollar estándares de seguridad organizacional y prácticas de gestión de seguridad efectivas y para ayudar a elaborar la confianza en las actividades inter-organizacionales. -Los requerimientos identificados por una evaluación de los riesgos, serán la base para la elaboración de los objetivos de control.

Fuente. Autores del proyecto

Basándonos en el estudio de las normas Cobit 4.1 – ISO/IEC 27001 – ISO/IEC 27002:

Para el planteamiento del SGSI del Área de contabilidad de la E.S.E se utilizará la norma ISO/IEC 27001, la cual contiene los requisitos básicos que debe tener todo sistema de gestión de seguridad de la información y es la norma sobre la cual se certifican, por auditores externos, los SGSI de las organizaciones. A pesar de no ser obligatoria la implementación de todos los controles, se debe argumentar la no aplicabilidad de los mismos. Se recomienda el uso del ciclo Plan – Do – Check – Act para el diseño de un SGSI.

Para el desarrollo de la Política de Seguridad de la Información base del SGSI, se seleccionó la norma ISO/IEC 27002, porque es un marco de trabajo de mejores prácticas internacionales que establece las guías y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en el Área de contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar. Sus objetivos de control y controles son recomendados para cubrir los requerimientos de seguridad que han salido de una evaluación de riesgos. ISO/IEC 27002 proporciona un lineamiento de implementación que se puede utilizar cuando se diseñan controles.

4.9 METODOLOGÍA PARA EL PLANTEAMIENTO DEL SGSI, EN EL ÁREA DE CONTABILIDAD DE LA E.S.E HOSPITAL LOCAL DE RIO DE ORO

Una de las principales características que debe poseer un empresa que busque establecer un SGSI es un enfoque por procesos, la norma ISO 27001 promueve la adopción del ciclo (Planear – Hacer – Verificar – Actuar) PHVA.

Con el fin de establecer una metodología general para la implementación de lo establecido en la norma ISO27001 para el Área de contabilidad de la E.S.E, seguiremos la metodología PHVA en la que enmarcaremos cada una de las etapas para la implementación del SGSI.

4.9.1 Definición del ciclo PHVA. El ciclo PHVA (o PDCA en ingles) es una herramienta de la mejora continua, diseñada por el Dr. Walter Shewhart en 1.920 y presentada por Deming a partir del año 1950, la cual se basa en un ciclo de 4 pasos: Planificar (Plan), Hacer (Do), Verificar (Check) y Actuar (Act)[23].

La metodología conocida como "Planificar- Hacer-Verificar-Actuar" (PHVA). PHVA puede describirse brevemente como:

[23] Plantilla para aplicar el ciclo PHVA. Tomado de: http://www.negociosyemprendimiento.org/2010/08/plantillapara-aplicar-el-ciclo-phva-de.html

-**Planear:** establecer los objetivos y los procesos necesarios para conseguir los resultados de acuerdo con los requisitos del cliente y las políticas de la organización.

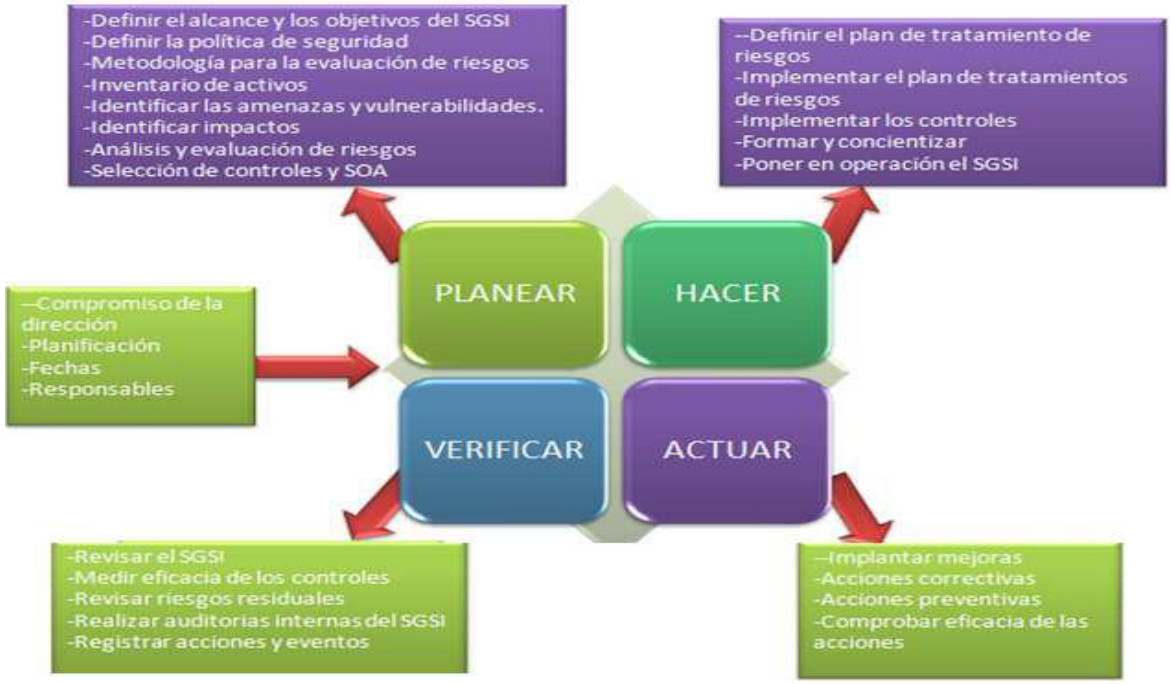
-**Hacer:** implementar los procesos.

-**Verificar:** realizar el seguimiento y medición de los procesos y los productos y servicios respecto a las políticas, los objetivos y los requisitos para el producto o servicio e informar los resultados.

-**Actuar:** tomar acciones para el mejoramiento continuo del desempeño de los procesos.

4.9.2 Ciclo PHVA PARA EL SGSI

Figura 14. Ciclo PHVA para el SGSI.



Fuente: http://www.iso27000.es/sgsi.html#section2d.

4.9.3 Arranque del proyecto. El compromiso de la dirección es la base fundamental para iniciar el proyecto, el apoyo y la decisión de implementar el SGSI debe ser una decisión de la dirección de la organización. El cambio cultural que se debe vivir junto con la aplicación de la norma es un proceso que necesita del impulso constante de la dirección. La norma ISO 27001 establece los compromisos que deben tener la dirección y la gestión de los recursos para lograr el funcionamiento del SGSI[24].

[24] ISO 27002:2005 Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información

- Los compromisos de la dirección se deben evidenciar mediante el establecimiento de una política, objetivos y planes del SGSI; establecer funciones y responsabilidades de seguridad de la información; comunicar a la organización la importancia del cumplimiento de lo establecido; brindar los recursos necesarios; decidir criterios y niveles para aceptación de riesgo; asegurar que se realicen las auditorías internas y efectuar las revisiones del SGSI.

- La dirección debe provisionar los recursos necesarios para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI; asegurar que los procedimientos de seguridad de la información brindan apoyo a los requisitos del negocio; identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales; mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados; llevar a cabo revisiones cuando sea necesario y mejorar la eficacia del SGSI.

4.9.4 Planear. En la etapa de planeación se define el alcance del sistema dentro de la organización y las políticas y lineamientos sobre los que se desarrollará, se presentan herramientas para la identificación, análisis y evaluación de riesgos, según el impacto de cada uno y el tipo de información que se afectaría, de igual forma es objetivo de esta etapa definir la forma de tratamiento de los riesgos identificados.

4.9.5 Alcance del SGSI. En primera medida la organización debe establecer el alcance del Sistema de Gestión de Seguridad en la Información SGSI, el alcance está en función de las características del negocio, la organización, localización, activos y tecnología por lo que definir el alcance no implica abarcar toda la organización, es más, es recomendable empezar por un alcance limitado, en el que se involucren los procesos *core* del negocio o que contengan la información más relevante para la compañía, es decir los que se han identificado en el mapa como misionales. Es indispensable disponer del mapa de procesos, e identificar claramente aquellos que harán parte de alcance.

Tener claro las terceras partes y su influencia sobre la seguridad de la información, es importante en el momento de definir el alcance, los requisitos legales y contractuales relacionados con la seguridad de la información deben quedar contemplados también dentro del alcance del sistema.

Cualquier otro proceso que la organización considere incluir dentro del SGSI es válido, lo que se recomienda es que la decisión de incluir más procesos sea con base en un análisis que en efecto sugiera la importancia de incluir dicho proceso, no se quiere hacer un SGSI muy robusto y poco efectivo, por el contrario, hacerlo lo más simple posible es una buena práctica, más aun cuando la organización empieza desde ceros el desarrollo del Sistema.

4.9.6 Política del SGSI. Diferentes teorías de administración convergen en que una clara definición de la razón de ser de una organización normalmente denominada Misión, acompañado de un objetivo ambicioso, cuantificable y explicito para un periodo de tiempo,

su Visión, es el pilar para poder desplegar las estrategias, procesos organizacionales y en general, para estructurar una empresa adecuada al cumplimiento de su propósito.

La política del SGSI entonces, debe estar alineada con los objetivos organizacionales, es allí donde la alta dirección debe establecer un marco de referencia para posteriormente fijar objetivos específicos de control por cada proceso de la compañía, los cuales deben establecerse en conjunto con el líder de cada proceso.

Figura 15. Política del SGSI.

Fuente: Los autores.

Parte fundamental en la implementación de sistema es la divulgación de la política trazada a toda la compañía con el fin de que las decisiones en los diferentes niveles de la compañía estén siempre alineadas con lo que la alta dirección espera del sistema, adicional, dejar clara la correlación o impacto de los objetivos genera mayor claridad de la razón de ser de los mismos y un mayor compromiso por parte de los responsables.

Finalmente la política debe contemplar los criterios y metodología para la valoración del riesgo, en donde se debe tener en cuenta lo siguiente:

- Determinar una metodología para la evaluación y clasificación de los riesgos que impactan la seguridad de la información.
- Identificar los riesgos
- Analizar y evaluar los riesgos encontrados
- Definir objetivos de Control y Controles para el tratamiento de riesgos
- Proponer opciones para el tratamiento de riesgos

La gestión de riesgo en la seguridad de la información, inicia al establecer el contexto, este se refiere a la definición del alcance, límites y la política del SGSI, con el fin de asegurar que todos los activos de información de la organización se contemplen en el SGSI. Es importante tener en consideración para los límites y criterios de aceptación de los riesgos: el tiempo, costo, recursos, impactos y requisitos legales para implementar los controles.
Al definir el contexto del SGSI, se realiza la valoración de los riesgos que involucra:

4.9.7 Identificación del riesgo. La identificación del riesgo contempla inicialmente la determinación de los activos de información dentro del alcance del SGSI, teniendo en cuenta la ubicación, responsable y funciones. De igual manera se deben determinar las amenazas, vulnerabilidades e impactos en la organización, por las posibles pérdidas de confiabilidad, integridad y disponibilidad sobre los activos.

Es importante tener claridad en los conceptos de amenaza y vulnerabilidad para identificarlas en el análisis de cada activo.

Amenaza: una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización. Ejemplo: acceso no autorizado, código malicioso, spam, hackers, hurto por empleados o no empleados, mal uso de los sistemas de procesamiento de la información, fraude, falla del sistema, negación del servicio, errores del usuario, desastres, etc.

Vulnerabilidad: la debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. Ejemplo: Falta de concientización, Falta de responsabilidades claras, Clasificación errónea de la información, Incapacidad de proporcionar evidencia, Falta de control de cambio o versión, Falta de mantenimiento, Identificación y autenticación inapropiada, Falta de seguridad de los medios, Falta de protección física, etc.

En el análisis de las amenazas y vulnerabilidades se requiere:

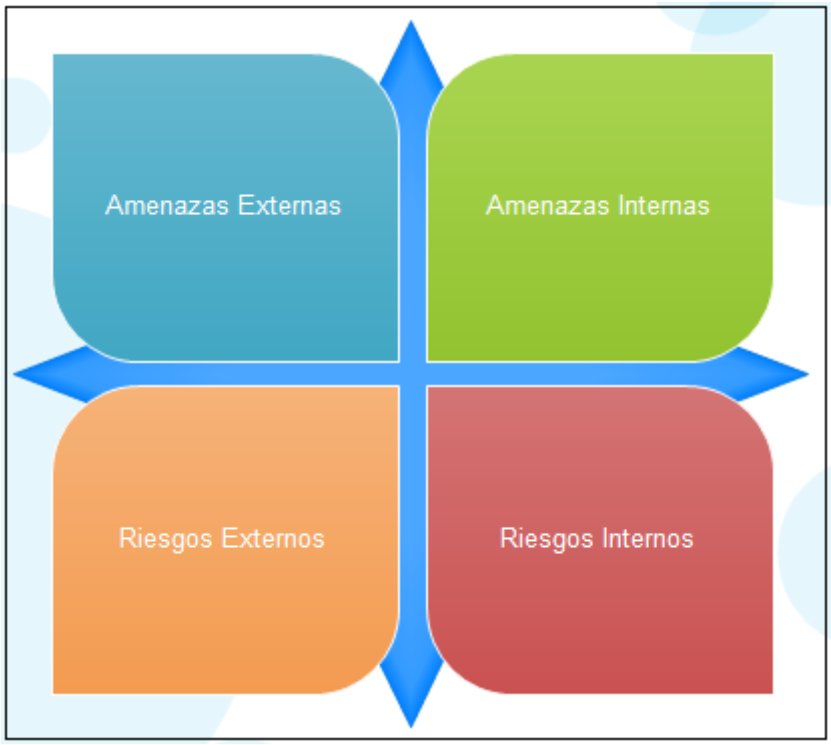
- Realizar una lista de las amenazas que puedan presentarse en forma accidental o intencional en la Empresa con relación a los activos de información. Diferenciar estas amenazas de las vulnerabilidades de los activos ya que el análisis debe radicar en las amenazas.

- Identificar los riesgos internos de los procesos analizando tanto las actividades que se desarrollan como las amenazas identificadas.

- Identificar los riesgos externos de los procesos. Es necesario analizar los riesgos que se pueden presentar cuando se subcontrata un servicio o existe personal externo a la organización.

- Realizar un análisis del entorno en los fenómenos naturales, el ambiente geopolítico, el ambiente tecnológico, el ambiente ecológico y los aspectos socioculturales que rodea la Organización para definir las amenazas a las que pueden estar expuestos los activos.

Figura 16. Amenazas y riesgos identificados el Área de contabilidad de la E.S.E.



Fuente. Los autores

4.9.8 Identificación del impacto. Una vez identificados los activos de información que posee la empresa para cada uno de los procesos que se han decidido incluir dentro del alcance del SGSI, se debe identificar cual sería el impacto que tendría en su respectivo proceso la pérdida o alteración de cada uno de los activos identificados.

Entiéndase impacto como el grado en el que se ve afectado determinado sistema, en este caso proceso, al alterar uno de sus componentes, para este caso activos de información. A mayor correlación entre el resultado del proceso y la alteración del activo, el impacto de ese activo será mayor.

Generalmente la evaluación del impacto viene de criterios subjetivos de los conocedores del proceso, en este documento se proponen 3 requisitos propios de los activos de información de una empresa, como lo describe la ISO 27001:2005 (Confidencialidad, Integridad y Disponibilidad), mediante los cuales se busca cuantificar el impacto que tiene dentro de su proceso.

Para cada requisito se han establecido 3 niveles de impacto (bajo, mediano y alto) según se comporte el activo dentro del proceso, se recomienda que en el momento de decidir cuál de los 3 niveles aplica para cada categoría, se conforme un grupo interdisciplinar y se de un espacio abierto para la discusión, la cuantificación final debe salir de un acuerdo general del grupo, el ejercicio debe hacerse tomando activo por activo, evaluando los 3 requisitos antes de continuar con el siguiente.

A continuación se describen los requisitos para hacer de la identificación del impacto como un ejercicio objetivo:

Tabla 6. Requisitos de Confidencialidad.

REQUISITOS DE CONFIDENCIALIDAD (C)		
VALOR DEL ACTIVO	CLASE	DESCRIPCIÓN
1. BAJO	Disponible al público	La información no sensible y las instalaciones de procesamiento de la información y los recursos del sistema están disponibles para el público
2. MEDIANO	Para uso interno exclusivamente o uso restringido solamente	La información no sensible está restringida para uso interno exclusivamente, es decir, no está disponible para el público o la información restringida y las instalaciones de procesamiento de la información y los recursos del sistema están disponibles dentro de la organización con restricciones variadas con base en las necesidades de la empresa.
3. ALTO	Confidencial o estrictamente confidencial	La información sensible y las instalaciones de procesamiento de la información y los recursos del sistema están disponibles sólo sobre la base de la necesidad del conocimiento, o la información sensible y las instalaciones de procesamiento de información y los recursos del sistema están disponibles sólo sobre la base de la necesidad estricta del conocimiento.

Fuente: Angelika Plate. ISO org. http://es.scribd.com/doc/24326153/29/ISO-IEC-27005-Anexos-Anexos

Tabla 7. Requisitos de integridad

REQUISITOS DE INTEGRIDAD (I)		
VALOR DEL ACTIVO	CLASE	DESCRIPCIÓN
1. BAJO	Baja integridad	El daño o modificación no autorizada no es crítico para las aplicaciones empresariales y el impacto en la empresa es insignificante o menor.
2. MEDIANO	Integridad mediana	El daño o modificación no autorizada no es crítico pero si es notorio para las aplicaciones empresariales y el impacto en la empresa es significativo.
3. ALTO	Integridad alta o muy alta	El daño o modificación no autorizada es crítica para las aplicaciones emresariales y el impacto en la empresa es importante y podría conllevar a la falta grave o total de la aplicación empresarial.

Fuente. Angelica Plate. ISO org. http:/es.scribd.com/doc/24326153/29/ISO-IEC-27005-Anexos-Anexos

Tabla 8. Requisitos de disponibilidad

REQUISITOS DE DISPONIBILIDAD (A)		
VALOR DEL ACTIVO	CLASE	DESCRIPCIÓN
1. BAJO	Baja disponibilidad	Se puedes tolerar que el activo no este disponible por más de un día.
2. MEDIANO	Disponibilidad mediana	Se puede tolerar que el activo no esté disponible por máximo de medio día a un día.
3. ALTO	Alta disponibilidad	No se puede tolerar que el activo no esté disponible por más de unas cuantas horas, o incluso menos.

Fuente. Angelica Plate. ISO org. http:/es.scribd.com/doc/24326153/29/ISO-IEC-27005-Anexos-Anexos

4.9.9 Análisis y evaluación del riesgo. La estimación del riesgo es el paso a seguir con el fin de valorarlo y determinar su importancia; puede ser cuantitativa al definir escalas de ocurrencia o cualitativa al usar escalas numéricas. El objetivo de esta etapa es obtener una lista de riesgos identificados de acuerdo a la probabilidad de ocurrencia de una amenaza y de sus consecuencias de los impactos, ligadas a las vulnerabilidades existentes a los activos de información. Por esta razón en la bibliografía se reporta que el riesgo en seguridad de la información se compone de tres elementos:

Riesgo= activo de información + probabilidad + impacto

Para esta etapa se propone utilizar los siguientes criterios de análisis y evaluación de riesgos

ANALISIS

IMPACTO / CONSECUENCIA	CUANTIFICACIÓN	DESCRIPCIÓN
Insignificante	1	· No hay daños o perjuicios.
		· La pérdida financiera es baja.
		· No hay pérdida de imagen.
Bajo	2	· Se puede subsanar los daños inmediatamente.
		· La pérdida financiera es media.
		· No hay pérdida de imagen.
Medio	3	· Se necesita asistencia de un tercero para subsanar los daños.
		· La pérdida financiera es alta.
		· Podría existir pérdida de imagen.
Grave	4	· Daños extensivos, pérdida de la capacidad de operación que no tiene efectos perjudiciales.
		· Pérdidas financieras mayores.
		· Pérdida de imagen
Muy grave	5	· Pérdida de la capacidad de operación que tiene efectos perjudiciales.
		· Enorme pérdida financiera.
		· Grave pérdida de imagen.

EVALUACION

IMPACTO / PROBABILIDAD		Insignificante	Bajo	Medio	Grave	Muy Grave
PROBABILIDAD		1	2	3	4	5
Muy probable	5	5	10	15	20	25
Probable	4	4	8	12	16	20
Factible	3	3	6	9	12	15
Remoto	2	2	4	6	8	10
Improbable	1	1	2	3	4	5

Nota: no se tendrán en cuenta la evaluacion como insignificante, se tomara como bajo

Riesgo Insignificante		
Riesgo Bajo		Gestionar mediante procedimientos de rutina, es improbable que se necesite la aplicación específica de recursos
Riesgo Moderado		Gestionar mediante procedimientos de monitoreo o respuesta específicas.
Riesgo Alto		Acción inmediata, especificar planes de acción y atención de la alta dirección.

PROBABILIDAD	CUANTIFICACIÓN	DESCRIPCIÓN	FRECUENCIA
Improbable	1	El evento ocurriría solamente en circunstancias excepcionales.	No se ha presentado en los últimos 5 años
Remoto	2	El evento podría ocurrir en algún momento y se considera que es difícil que suceda.	Al menos 1 vez en los últimos 5 años
Factible	3	El evento puede suceder eventualmente.	Al menos 1 vez en los últimos 2 años
Probable	4	El evento probablemente ocurrirá.	Al menos 1 vez en el último año
Muy probable	5	Se espera que el evento ocurra en la mayoría de los casos.	Más de 1 vez al año.

IMPACTO DE LA CONSECUENCIA POSITIVA	CUANTIFICACION	DESCRIPCION
Insignificante	1	Ganancias financieras pequeñas.
Menor	2	Ganancia financiera media.
Moderada	3	Ganancia financiera alta.
Importante	4	Ganancias financieras considerables.
Mayor	5	Ganancia financiera enorme.

4.9.10 Hacer. Siguiendo la metodología del PHVA, trataremos en este punto el desarrollo del paso HACER, inicialmente se debe definir el plan de tratamiento de los riesgos que se identificaron en el punto anterior, la manera de gestionar estos riesgos y la selección y aplicación de los controles para mitigarlos. Cuando se implemente el plan de tratamiento y los controles se debe alcanzar los objetivos de control que se identificaron en el planear.

Para el desarrollo de este punto es necesario tomar como punto de referencia la norma ISO 27001:2005 la cual establece las directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en la organización. Como segundo paso se debe empezar con una toma de conciencia y formación de todo el personal de la organización en lo relativo a la seguridad de la información. Si este paso no se lleva a cabo el SGSI no va tener ningún sentido y no va generar los beneficios de la implementación, para lograr esto sugerimos desarrollar el marco normativo necesario, las normas, los manuales, los procedimientos e instrucciones que permitan gestionar las operaciones del SGSI y los recursos asignados además recomendamos implementar procedimientos y controles de detección y respuesta a incidentes de seguridad que van a evaluar la efectividad de los controles en funcionamiento.

Teniendo en cuenta lo anterior el HACER contempla[25]:

- Definir el plan de tratamiento de riesgos
- Implementar el plan de tratamientos de riesgos

[25]ISO 27002:2005 Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.

- Implementar los controles
- Formar y concientizar
- Poner en operación el SGSI.

4.9.11 Plan de tratamiento del riesgo. La gestión de los riesgos es un proceso en el cual se implementan las medidas técnicas y organizativas necesarias para impedir, reducir o controlar los riesgos analizados e identificados, de forma que las consecuencias que puedan generar sean eliminadas o, si esto no es posible, se puedan reducir lo máximo posible. Un resultado del análisis de riesgos es el criterio para determinar los niveles de riesgo aceptables y en consecuencia, cuáles son los niveles inaceptables y que por lo tanto serán gestionados. El objetivo es reducir los riesgos que estén por encima de los niveles aceptables, a niveles que puedan ser asumidos por la organización[26].

Figura 17. Tratamiento del riesgo en el SGSI.

Fuente: Poveda, J. Gestión y tratamiento de los riesgos, 2007.

Una vez se han analizados y se conocen los riesgos de la organización se determinara el tratamiento que deben recibir los activos y se deben tomar las acciones necesarias. Los cuatro tipos de tratamiento requieren de diferentes acciones:

- **Mitigar el riesgo:** Reducirlo mediante la implantación de controles que reduzcan el riesgo a un nivel aceptable, implica seleccionar dichos controles, definir y documentar los métodos para ponerlos en marcha y gestionarlos.

[26] Poveda, J. Gestión y tratamiento de los riesgos, 2007. http://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-9.pdf.

- **Asumir el riesgo:** La Dirección asume el riesgo ya que está por debajo de un valor de riesgo aceptable, simplemente requiere que quede documentado que la dirección conoce y acepta estos riesgos. Los riesgos que se han asumido han de ser controlados y revisados periódicamente de cara a evitar que evolucionen y se conviertan en riesgos mayores.

- **Transferir el riesgo a un tercero:** Como por ejemplo, asegurando el activo que tiene el riesgo o subcontratando el servicio. Deben evaluarse las opciones y tomar las acciones pertinentes para ejecutar la opción escogida, en función del valor del activo y del coste de realizar esta transferencia (no sólo coste económico sino también los riesgos que conlleva esta transferencia en cuanto a la inclusión de un tercero).

- **Eliminar el riesgo:** Aunque no suele ser la opción más viable, ya que puede resultar difícil o demasiado costoso, si se cree posible o necesario, habrá que establecer los pasos para conseguirlo: eliminar el activo, eliminar el proceso o incluso el área de negocio que es la fuente del riesgo.

No habrá más acciones a la hora de gestionar los riesgos para la correcta implantación de un sistema de gestión de la seguridad de la información, ya que una organización que conoce sus riesgos jamás podrá ignorarlos, puesto que, de este modo, no estaría vigilando y daría lugar a un incidente de seguridad.

4.9.12 Mitigación del riesgo. Una vez se han identificado los requisitos y los riesgos de seguridad y se han tomado las decisiones para el tratamiento de los riesgos, es conveniente seleccionar e implementar los controles para garantizar la reducción de los riesgos hasta un nivel aceptable. Los controles se pueden seleccionar a partir de la norma ISO 27002:2008.

PASOS PARA MITIGAR EL RIESGO:

- Seleccionar los controles apropiados para los riesgos que se han analizado y se determino tratar, en principio del Catálogo de Buenas Prácticas de la ISO/IEC 27002 (133 controles posibles).

- Diseñar los procedimientos para implantar los controles aunque sean controles técnicos es necesario procedimiento de instalación, uso y mantenimiento.

- Verificar que los controles estén correctamente implantados.

- Establecer indicadores que permitan medir la implementación de los controles y si reduce el riesgo al nivel de aceptación.

4.9.13 Selección de controles. Los controles se seleccionarán e implementarán para minimizar en lo posible la posibilidad de que los riesgos detectados en el análisis de riesgos dañen los activos. Existen dos grandes grupos de controles. Por un lado los técnicos, tales como sistemas de cifrado, copias de seguridad, sistemas de detección de intrusos,

actualizaciones de software, antivirus o cortafuegos, y por otro los organizativos que son medidas organizativas tales como la Política de Seguridad, procedimientos de uso de los sistemas de información para los usuarios, los planes de formación o los planes de continuidad del negocio.

4.9.14 Implementación de controles. Seleccionados los controles pertinentes, debe definirse los procedimientos para su implantación. Los controles de tipo organizativo se prestan más a ser implantados mediante procedimientos, como por ejemplo la gestión de los recursos humanos. Pero incluso los de corte tecnológico pueden ser susceptibles de necesitar documentación, como por ejemplo la realización de copias de seguridad. Debe analizarse la lista de controles seleccionados y establecer qué procedimientos necesitan ser desarrollados.

4.9.15 Verificación de controles. Una vez puestos en marcha, debe comprobarse periódicamente que los controles funcionan como se esperaba. Si no es así, deberán tomarse las acciones necesarias para corregir esa situación. Una herramienta fundamental del SGSI es la verificación de la eficacia de los controles implantados. Para ello deben establecerse objetivos de rendimiento para los controles, marcar puntos de control y medición y registrar los resultados de manera que se sepa si el control realmente protege los activos hasta el punto que la organización necesita.

4.9.16 Documentación del plan de tratamiento de riesgos. La documentación de la gestión de riesgos se realiza mediante la Declaración de Aplicabilidad también conocida por sus siglas en inglés SOA ("Statement Of Applicability"). Este documento, requerido por la Norma UNE/ISO-IEC 27001, es un resumen de las decisiones que se han tomado para tratar los riesgos analizados y debe incluir los 133 controles de la ISO/IEC 27002.

Para cada uno de los controles debe reflejarse en este documento[27]:
- Si está implantado actualmente en la organización, con una breve descripción de cómo se aplica.

- Si se va a implantar, es decir, si es uno de los controles escogidos para mitigar el riesgo, junto con las razones para haberlo seleccionado.

- Si no se va a implantar, y entonces hay que exponer los motivos que han llevado a esta decisión. Las exclusiones deben justificarse adecuadamente.

Este documento constituye de alguna manera un registro de los resultados finales del SGSI, ya que concreta de manera clara y directa en qué va a consistir el sistema de seguridad, detallando cada uno de los controles que se tiene la intención de aplicar de manera explícita.

[27] ISO 27002:2005 Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.

4.9.17 Controles e implementación para el área de contabilidad de la E.S.E.[28]

A continuación se relacionan las principales medidas de seguridad relacionadas directamente con el Área de contabilidad, tomando como base la norma ISO/IEC 27002.

4.9.17.1 Definición de la política de seguridad del área de contabilidad

Después de un análisis realizado a la norma ISO/IEC27002 y teniendo en cuenta las necesidades de Área de contabilidad en la implementación de buenas prácticas para la gestión de la seguridad de la información, se determinó que de los once dominios establecidos en la norma solo se tendrán en cuenta 10 los cuales se definen a continuación:

1. Política de seguridad

Objetivo de control: Política de seguridad de la información
Controles:
- Documento de la política de la seguridad de la información
- Revisión de la política de seguridad de la información

2. Organización de la Seguridad Informática

Objetivo de control: Organización interna
Controles:
- Coordinación de la seguridad de la información.
- Asignación de responsabilidades para la seguridad de la información.

3. Gestión de Activos

Objetivo de control: Responsabilidad por los activos
Controles:
- Inventario de activos
- Uso aceptable de los activos

4. Seguridad ligada a los recursos humanos

Objetivo de control: Antes de la contratación laboral
Control:
- Términos y condiciones laborales

Objetivo de control: Durante la vigencia del contrato laboral

[28] ISO 27002:2005 Tecnología de la Información – Técnicas de seguridad – Código parala práctica de la gestión de la seguridad de la información.

Controles:

- Educación, formación, y concientización sobre la seguridad de la información
- Proceso disciplinario

Objetivo de control: Terminación o cambio de la contratación laboral
Control:
- Devolución de activos

5. Seguridad física y del entorno

Objetivo de control: Áreas seguras
Controles:

- Perímetro de seguridad física
- Controles de acceso físico
- Protección de amenazas externas y de origen ambiental
- Trabajo en áreas seguras

Objetivo de Control: Seguridad del equipo
Controles:

- Ubicación y protección del equipo
- Mantenimiento de quipo
- Seguridad del equipo fuera del local
- Traslado de propiedad

6. Gestión de comunicaciones y operaciones

Objetivo de control: Procesamientos y responsabilidades operacionales
Controles:

- Procesamiento de operación de documentos
- Gestión de cambio
- Separación de los medios de desarrollo y operaciones

Objetivo de control: Planeación y aceptación del sistema
Control:

- Controles contra software malicioso

Objetivo de control: Respaldo (back-up)
Control:

- Back-up o respaldo de la información

Objetivo de control: Gestión de seguridad de redes
Control:
- Controles de red

Objetivo de control: Gestión de medios
Control:

- Gestión de los medios removibles

7. Control de acceso

Objetivo de control: Gestión del acceso de usuarios
Controles:

- Inscripción del usuario
- Gestión de la clave del usuario
- Política de pantalla y escritorio limpio

Objetivo de control: Control de acceso a redes
Control:

- Política sobre el uso de servicios en red

8. Adquisición, desarrollo y mantenimiento de sistemas de información

Objetivo de control: Seguridad de los archivos del sistema
Controles:

- Control de software operativo

Objetivo de control: Seguridad en los procesos de desarrollo y soporte
Controles:

- Procedimiento de control de cambios

9. Gestión de incidentes en la seguridad de la información

Objetivo de control: Reporte sobre los eventos y las debilidades de la seguridad de la información
Control:

- Reporte sobre los eventos de seguridad de la información

Objetivo de control: Gestión de los incidentes y las mejoras en la seguridad de la información

Control:

- Aprendizaje debido a los incidentes de seguridad de la información

10. Cumplimiento

Objetivo de control: Cumplimiento de los requisitos legales.
Controles:

- Identificación de la legislación aplicable.
- Protección de los datos y privacidad de la información personal.

Los dominios que no son implementados en el manual de la política de seguridad de la información **Gestión de continuidad del negocio** ya que éste consiste en la protección de procesos y recursos del negocio, permitiendo también minimizar la perdida de activos en desastres naturales, accidente, fallas del equipo y acciones deliberadas. Es por ello que la alta gerencia como principal responsable de cumplir con los objetivos del negocio debe asumir el diseño, implantación y mantenimiento del plan de continuidad como un elemento fundamental como el éxito de su gestión; por ésta razón en la política de seguridad no se incluye este dominio ya que debe ser diseñada e implementada para toda la E.S.E, en este caso El Hospital Local de Rio de Oro Cesar y no solo para el Área de contabilidad.

4.9.18 Formación, toma de conciencia y competencia. Como último paso en el HACER, la norma ISO 27001 establece que la organización debe asegurar que todo el personal que tenga responsabilidades con el SGSI debe ser competente para cumplir sus tareas. Para garantizar sus competencias la E.S.E debe determinar las competencias necesarias de los colaboradores, realizar actividades de formación o contratar personal si es necesario, evaluar la eficacia de las acciones que se están realizando y mantener registros de las formaciones, habilidades, experiencia y calificaciones[29].

4.9.19 Objetivos de control e indicadores. La Norma estipula que se deben incluir las acciones que se van a realizar para gestionar el riesgo en el plan de tratamiento. Estas acciones serán parte de la mejora continua del SGSI y se debe medir, estableciendo objetivos e identificando las oportunidades de mejora. Una vez establecidos los objetivos, se debe establecer los indicadores de rendimiento para medir el cumplimiento de los objetivos. Para poder medir es necesaria la información que se recogerá a partir de los registros del sistema reflejados en cada uno de los documentos, para realizar una medición adecuada la información debe ser pertinente, precisa y oportuna.

[29] ISO 27002:2005 Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.

Es importante realizar un control del indicador para determinar si es adecuado para la información que se quiere obtener. Si no cumple con los criterios de selección es necesario definir nuevos indicadores[30].

4.9.20 Verificar. Una vez que está en marcha el SGSI es fundamental hacer un seguimiento de cómo funciona y cómo va evolucionando el sistema. En primer lugar para corregir las posibles desviaciones sobre lo planificado y previsto y en segundo lugar, aunque igual de importante, detectar oportunidades de mejora del sistema, ya que el objetivo último de implantar un sistema de gestión de este tipo es el mejorar continuamente, hacer cada vez más con los limitados recursos disponibles.

4.9.21 Revisión del SGSI. Uno de los requisitos más relevantes de la Norma ISO 27001 es la revisión que la dirección de la organización debe realizar con una cierta periodicidad, como mínimo anual, al Sistema de Gestión de Seguridad de la Información. Esta revisión tiene como objetivo asegurarse de que el SGSI es en todo momento adecuado, apropiado y efectivo para los propósitos y contexto de la organización. Esta revisión forma parte de la fase VERIFICAR del ciclo de mejora continua, y es una herramienta magnífica para el análisis y la adopción de oportunidades de mejora, ya que se contemplan todos los aspectos y la marcha del SGSI, por lo que se tiene una visión general de todo y se pueden detectar los puntos débiles y discutir sobre cómo mejorarlos. Existen muchas formas en que la alta dirección puede revisar el SGSI como, por ejemplo, recibir y revisar un informe generado por el representante de la dirección u otro personal, o incluir los temas pertinentes en la agenda de reuniones regulares de la dirección[31].

Entradas para el proceso:

Existen muchas fuentes de las que se pueden recoger datos e información útiles para realizar la revisión por la dirección:

Las auditorías llevadas a cabo en la organización. No sólo las auditorías internas del SGSI son útiles aquí, sino también otras auditorías tales como auditorías de clientes, de otras normas de gestión, etc. Todas ellas pueden aportar información sobre los puntos fuertes y débiles del SGSI y poner en evidencia oportunidades de mejora.

Las anteriores revisiones del SGSI y las acciones derivadas del mismo, son el punto de partida, dónde estaba el SGSI y qué es lo que se ha hecho al respecto desde entonces.

Analizar qué se decidió hacer y hasta donde se ha avanzado, proporciona información muy valiosa sobre qué se puede hacer para continuar mejorando y progresando.

[30] Metodología línea base de indicadores. DANE 2009.
[31] ISO 27002:2005 Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.

Estudiar por qué no se han llevado a cabo todas las acciones planificadas servirá para detectar puntos débiles y obliga a determinar nuevas medidas.

Comentarios de las partes interesadas. A lo largo de la actividad cotidiana de la organización, tanto clientes, como usuarios, proveedores, público, cualquiera que entra en contacto con ella puede emitir algún comentario que puede ser útil para diseñar alguna acción de mejora. Debe existir algún mecanismo, aunque sea informal para incorporar esta información al sistema.

Técnicas, productos o procedimientos, que podrían ser usados en la organización para mejorar el funcionamiento y la efectividad del SGSI. La información necesaria para este punto probablemente vendrá en primer lugar del responsable de sistemas, pero también las distintas personas involucradas en tareas que necesiten mejoras pueden aportar ideas al respecto.

El estado de las acciones preventivas y correctoras. Hay que analizar las acciones, que son la medida de cómo se desarrolla la actividad cotidiana del SGSI, estudiando cuantas se han abierto, por qué motivo, si se han ido cerrando en plazo, si ha habido problemas con alguna de ellas, etc. Con esa información se extraerán conclusiones importantes para la mejora del SGSI.

Las vulnerabilidades o amenazas que no se han tratado adecuadamente en análisis de riesgos anteriores. Es decir, si se han detectado nuevas amenazas o ha habido cambios que necesiten revisar las anteriormente consideradas, o bien valorar si riesgos que no se trataron por cualquier motivo antes, ahora necesitan de tratamiento.

La evaluación de los objetivos. Uno de los principales puntos de esta revisión es comprobar si se han conseguido los objetivos marcados en un principio. Cuando se diseña el SGSI, se marcan unos objetivos, para los que habrá que definir unas métricas que permitan evaluar hasta qué punto se han alcanzado los objetivos. Esta información es la que indica si el SGSI funciona o no, si es eficaz o no. A la luz de esta información se podrá decidir si hay que modificar los objetivos o qué acciones tomar para alcanzarlos.

Cambios en la organización. Cambios por ejemplo en la infraestructura informática por ejemplo, que afectaría de manera directa y clara al SGSI, ya que las medidas de seguridad aplicadas en los anteriores sistemas de información pueden no ser válidas o suficientes para los nuevos sistemas. Pero también cambios en el personal, que requieran reajustar los privilegios en el acceso a la información, en los servicios que la organización ofrece, que pueden plantear nuevos requisitos de seguridad, etc.

Salidas del proceso:

Mejoras de la efectividad del SGSI, es decir, qué se va a hacer para mejorar el SGSI: se van a implantar más controles, se van a mejorar los ya implantados, se van a transferir riesgos, etc.

Actualización de la evaluación y gestión de riesgos. Hay que documentar los cambios que se hayan producido en el análisis y gestión de los riesgos y los motivos que los han motivado.

Modificación de procedimientos y controles que afectan a la seguridad de la información, según sea necesario, para responder a incidentes internos o externos que puedan impactar en el SGSI, incluyendo cambios en:

Requisitos de negocio, de seguridad o legales.

Procesos de negocio que tengan efecto en los requisitos de negocio existentes.

Obligaciones contractuales.

Cambios en el nivel de riesgo aceptable.

Necesidades de recursos.

Mejoras en la manera de medir la efectividad de los controles. Al revisar los indicadores que se utilizan debe comprobarse si siguen siendo útiles, eliminando aquellos que no lo sean y diseñando nuevos indicadores más eficaces a la hora de suministrar información relevante.

4.9.22 Herramientas propuestas. En la etapa del verificar es viable implementar herramientas como cartas de control, planes de verificación del SGSI, balanced scorecard o cuadro de mando integral y el programa de auditorías internas, entre otros, que faciliten realizar el seguimiento del SGSI y determinar su cumplimiento de acuerdo a la ISO 27001.

De una manera práctica el Plan de verificación permite identificar los riesgos que no se están tratando correctamente en el SGSI por múltiples causas o variables, al conocer el consolidado de los indicadores. Por lo tanto brinda la información para tomar decisiones y determinar las acciones preventivas o correctivas correspondientes (Actuar). Además de ser una herramienta para evaluar periódicamente los procesos y controlar la residualidad de los riesgos al determinar si los métodos de control no son eficientes y eficaces.

4.9.23 Auditorias internas. Podemos definir auditoría como una actividad independiente que tiene lugar dentro de la organización y que está encaminada a la revisión de operaciones con la finalidad de prestar un servicio a la dirección, ya que en realidad es un control de dirección El objetivo de una auditoría es determinar si los objetivos de los controles, los controles, los procesos y los procedimientos están conformes con los requisitos de la Norma en la que se audite el sistema, los requisitos legales y reglamentarios, los requisitos de la organización (contractuales, de seguridad, internos, etc.). Además de esto, la auditoría verifica si el SGSI se mantiene de manera efectiva y se obtienen los resultados esperados. Es decir, si el sistema dice lo que hace y hace lo que

dice. La planificación de la auditoría debe hacerse al menos anualmente, ya que es importante realizar una revisión al sistema completo a lo largo del año, decidiendo no solo las fechas en las que se va a realizar, sino si el alcance va a ser global o parcial y en este último caso, las áreas y procesos que van a ser auditados en cada una de las auditorías. Una vez hecho esto, se puede comenzar a preparar la auditoría en sí, decidir los criterios de auditoría, el método que se va a utilizar e informar a los afectados por la auditoría con tiempo suficiente para que se puedan preparar. .

Las personas que asuman el rol de auditor Interno tienen que poseer la necesaria preparación profesional en las metodologías que hay que emplear, los conocimientos generales (tanto del ambiente empresarial como del SGSI) y contar con el carisma personal para tener credibilidad y el respaldo de la dirección. Es muy importante que sean personas que tengan independencia en relación con las actividades involucradas. Los resultados de una auditoría realizada por alguien que realiza o controla el trabajo auditado estarán probablemente sesgados, por lo que debe evitarse esta situación.

4.10 ACTUAR

La implantación del SGSI debe ser un proceso dinámico, para esta etapa debe estar claro que la misión del SGSI es situar la seguridad de la información al mismo nivel que cualquier otro objetivo de negocio, y como tal, debe ser optimizado continuamente. Esta etapa corresponde al Capítulo 8 de la ISO 27002. Es en esta fase cuando deberemos implantar las medidas correctivas fruto de las revisiones efectuadas, y mejorar así el rendimiento del SGSI. Las medidas correctivas comprenden la selección de nuevos controles, la modificación de los existentes o la eliminación de los obsoletos. Resulta bastante frecuente que se haga necesario rectificar el alcance inicial del SGSI y su diseño[32].

Es así que en esta etapa deberá tenerse en cuenta:

1. Identificar no conformidades del SGSI.
2. Realizar análisis de causa raíz
3. Definir acciones correctivas y preventivas.
4. Identificar las mejoras potenciales del SGSI que se hayan propuesto en la fase anterior y ponerlas en marcha.
5. De ser necesario, obtener el visto bueno de la Dirección para la implementación de los cambios propuestos y aprobación de recursos necesarios
6. Divulgar o comunicar las acciones y mejoras a todos los interesados.
7. Evaluar la efectividad del plan de mejora continua tomando como base los resultados obtenidos de las acciones implementadas y realizar planes de acción concretos para mejorar el SGSI.

[32] ISO 27002:2005 Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.

Entradas para el proceso:

1. Informes de Auditoría interna.
2. Informes de no conformidades.
3. Informes de conclusiones y sugerencias que surjan de la etapa de revisión.
4. Propuestas de mejoras de otras áreas y unidades de negocios.

Personas responsables

1. Equipo de Planeamiento de la Seguridad de la información, responsable de sugerir las mejoras que pueden obtenerse y estimar los recursos que serían necesarios.
2. Alta Gerencia en caso de ser los cambios propuestos de un impacto considerable o requerir presupuesto adicional al ya otorgado.

Salida del proceso:

Un Informe con el plan de mejoras, describiendo o referenciando las conclusiones más relevantes surgidas de la etapa de revisión y especificando objetivos concretos, el impacto de los cambios y quienes estarían involucrados así como un plan tentativo para llevarlos a cabo.

4.10.1 Herramientas propuestas. Existen diversas herramientas que se han desarrollado con el fin de ayudar a establecer planes de acción efectivos al momento de resolver un problema dentro de una organización.

4.10.2 Acciones correctivas y preventivas. Cuando se producen no conformidades, es decir, cuando hay un incumplimiento de un requisito, bien de la Norma bien de las pautas internas, se deben toman acciones encaminadas a resolver esa situación no deseada. Las acciones contempladas por la Norma se dividen en:

Acciones correctivas.
Acciones preventivas.
Acciones de mejora.

Las acciones correctivas son las que se toman para corregir una no-conformidad significativa con los requisitos del Sistema de Gestión de Seguridad de la Información. Se pueden detectar no conformidades durante cualquiera de las auditorías y revisiones a las que se somete el SGSI, al analizar los registros de incidencias, ya las que sean graves o reiteradas en el tiempo constituyen no conformidades, o durante la operativa habitual del SGSI[33].

[33]ISO 27002:2005 Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.

Las acciones preventivas como su propio nombre indica, son aquellas que se toman para eliminar la causa de una posible no conformidad, es decir, se actúa antes de que ocurra. En una acción preventiva se determina la posible fuente de problemas antes de se haya materializado, con el objeto de eliminarla y evitar que se produzca.

En ambos casos, para abrir una acción es necesario recoger todos los datos e información relativos al problema a tratar. A partir de ahí se trata de determinar el origen del problema y las primeras acciones a tomar, los responsables de ejecutar estas acciones y los plazos para ello.

Para cerrar una acción debe verificarse que se ha resuelto satisfactoriamente, es decir que ha sido efectiva.

Cuando se deciden acciones que no están relacionadas con una no conformidad éstas se denominan acciones de mejora. Pueden venir de sugerencias del personal, de la revisión del SGSI, etc. Estas acciones suponen un cambio positivo en la manera de afrontar una tarea o procesos de manera que se mejoren la operativa, los resultados o ambas.

4.11 DOCUMENTACIÓN DEL SGSI

Basados en la norma ISO 27001 se tendrá documentación desde nivel 1 hasta nivel 4 donde se incluyen el manual de seguridad, los procedimientos, los formularios y los registros.

Adicional a esto se tendrán los documentos que enmarcan el SGSI y el control que se debe tener de los mismos.

- **Documentos de nivel 1**

Manual de seguridad: es el documento que inspira y enmarca el sistema, expone y especifica las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales. Es un análogo al manual de calidad.

- **Documentos de nivel 2**

Procedimientos: son la estandarización de los procesos operativos que aseguran el cumplimiento de la planificación, operación y control de los procesos de seguridad de la información de una forma eficaz.

- **Documentos de nivel 3**

Formularios: también conocidos como checklist o instrucciones los cuales describen las tareas y actividades específicas relacionadas con la seguridad de la información.

- **Documentos de nivel 4**

Registros: documentos que proporcionan evidencia del cumplimiento de los requisitos, están asociados a documentos de los otros niveles como elemento de salida que demuestra el cumplimiento de lo que se estipula en los mismos.

- **Documentos específicos del SGSI**

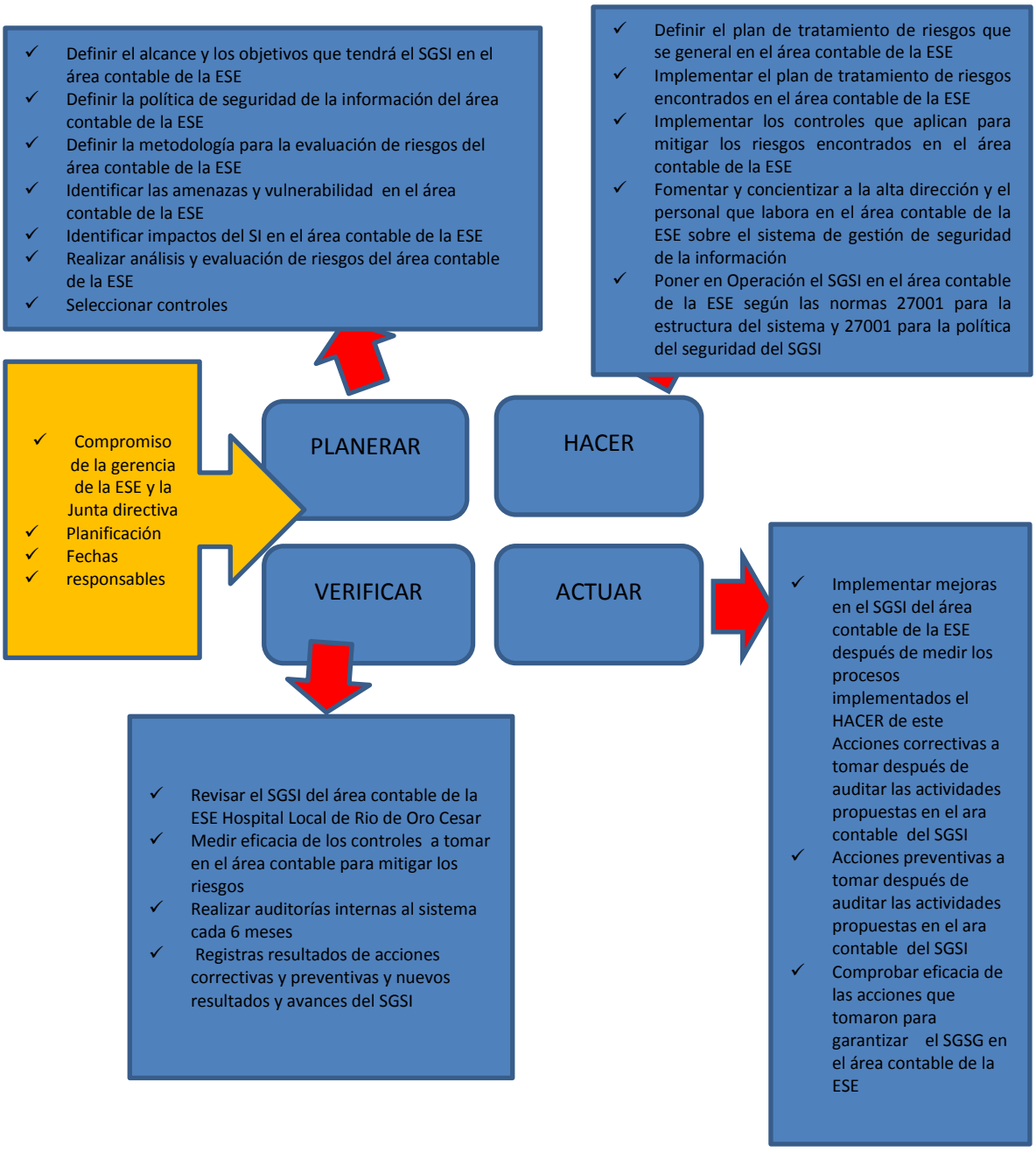
De manera específica ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos: Alcance del SGSI, Política y objetivos de seguridad, Procedimientos y mecanismos de control que soportan al SGSI, Enfoque e informe de evaluación de riesgos, Plan de tratamiento de riesgos y Declaración de aplicabilidad

- **Control de documentos**

Para todos los documentos que se generen en el SGSI se debe establecer, documentar, implementar y mantener un procedimiento que defina cuales es la gestión para: aprobar documentos, revisar y actualiza documentos, garantizar la identificación de los cambios y el estado actual de revisión de los documentos, la vigencia de los documentos y la disponibilidad para el lugar donde se utiliza, garantizar que los documentos se mantengan legibles y fácilmente identificables, el control de la distribución de los documentos, prevenir el uso de los documentos obsoletos e identificar los documentos que son retenidos. Se deben establecer y mantener registros para brindar evidencia de la conformidad con los requisitos y la operación eficaz del SGSI.

4.12 DOCUMENTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DEL ÁREA DE CONTABILIDAD, INCORPORANDO LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

4.12.1 Ciclo PHVA para el SGSI del área contable de la ESE Hospital local de Rio de Oro



1. MISION:

Cumplimos procesos organizados, dignos, oportunos y confiables el mejoramiento de la calidad de vida de los usuarios y la atención adecuada y a tiempo en cada uno de los servicios de la ESE desde el área financiera y contable ayudando a solucionar los problemas que se presenten y ser eficaces en la organización.

2. VISION

Ser un área con ética, innovador y de una excelencia contable optima enfocada al servicio de la administración para el beneficio dl sector salud del municipio de Rio de Oro conservando el reconocimiento a nivel departamental, regional y nacional.

3. OBJETIVOS

- Revisar, inspeccionar y dar cumplimiento del estado general de la seguridad de la información y Política de Seguridad del área contable de la ESE Hospital Local de Rio de Oro Cesar.

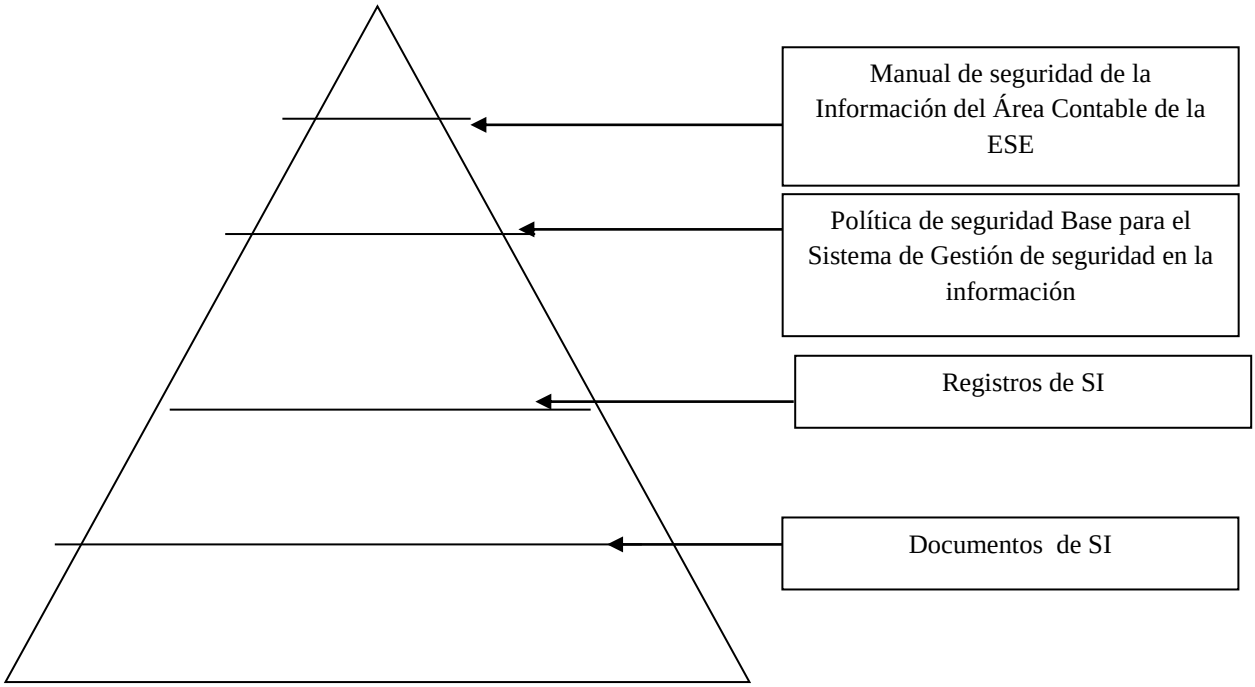
- Implementar nuevas políticas y análisis de riesgos de seguridad de la información del área contable de la ESE Hospital Local de Rio de Oro Cesar.

- Mejorar Continuamente el SGSI en el área contable de la ESE Hospital Local de Rio de Oro Cesar

4. ESTRUCTURA DE LA DOCUMENTACIÓN

La ESE Hospital Local de Rio de Oro Cesar ha consignado la documentación necesaria para el Sistema de Gestión de Seguridad de la Información, un manual de procedimientos para garantizar la seguridad de la información en el are contable de la ESE y de apoyo también para garantizar el seguridad de la información en el área contable.

PIRÁMIDE DOCUMENTAL DE SGSI



El **Manual de Seguridad de la Información del área contable de la ESE hospital Local de Rio De Oro Cesar** hace referencia a la forma en que la organización responde a los requisitos de la norma **ISO 27001-2005**. Este manual incluye la misión, visión, la política de seguridad de la información y los objetivos de seguridad de la información, el alcance de nuestro sistema y los detalles justificativos de las exclusiones.

Seguidamente, en el anexo **Caracterizaciones de los Procesos**, se establece una ficha técnica y un flujo grama característico de cada proceso. La caracterización de los procesos define la forma como la Institución determina los criterios y métodos para asegurar que nuestra área de contabilidad garantizara la seguridad de la información de sus procesos.

También garantiza este manual que se implementan las acciones necesarias para alcanzar los resultados planificados y la mejora continúa el sistema de inofmacion del area contable.

El **Mapa de Procesos** de la organización se encuentra incluido en el Manual de seguridad de la información y en él se muestra de manera genérica la interacción entre los procesos del sistema de gestión de seguridad de la infomacion en el área contable de la ESE

Los **Registros** presentan evidencia objetiva de las actividades efectuadas .Los **Documentos** presentan aquellos documentos externos que utiliza la organización para el desarrollo de sus actividades.

5. POLITICA DE SEGURIDAD DE LA INFORMACIÓN BASE PARA EL SGSI

POLÍTICA DE SEGURIDAD

La Política de seguridad establece las acciones necesarias y los procedimientos para garantizar la confidencialidad, integridad y disponibilidad de la información, así como los mecanismos utilizados para la implementación de los mismos.

Debe dedicarse un tiempo significativo para la creación de la Política de Seguridad de la Información de la empresa, proceso que estará orientado por el Comité de Seguridad de la información.

A continuación se desarrollará la Política de Seguridad de la Información para el Área de contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar:

6. RESOLUCIÓN NO. 001 DE 2014

Por la cual se regulan las políticas de seguridad de la información y el uso adecuado de la tecnología para el procesamiento de la información en el Área de contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar.

EL JEFE DEL ÁREA DE CONTABILIDAD DE LA E.S.E HOSPITAL LOCAL DE RIO DE ORO CESAR

En uso de sus facultades legales y estatutarias y

CONSIDERANDO

Que el Área de contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar, reconoce que la información es un activo valioso y que se requieren políticas adecuadas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la misma.

Que la Constitución Política en su Artículo 61 establece que el Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley.

Que el Área de contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar debe promover y proteger la producción intelectual de los miembros de su comunidad mediante el reconocimiento debido de los derechos morales y patrimoniales generados.

Que se hace necesario el establecimiento de las políticas de seguridad de la información que protejan, preserven y administren correctamente la información del Área de contabilidad de la E.S.E, junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información. Que en mérito de lo expuesto.

RESUELVE:

CAPÍTULO I

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información del Área de Contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar estará integrado por:

- Gerente (Coordinador del Comité de Seguridad de la Información)
- Ingeniero de Sistemas (Responsable de los sistemas de información)
- Jefe del Área de contabilidad (Responsable de los procesos contables)
- Jefe de Recursos Humanos (Responsable del Área de Recursos Humanos)

Los integrantes del Comité velarán por el cumplimiento de los siguientes objetivos de seguridad:

- ✓ Revisar el estado general de la seguridad de la información periódicamente.
- ✓ Inspeccionar y monitorear los incidentes de seguridad de la información.
- ✓ Dar cumplimiento a las políticas de seguridad que se hayan establecido.
- ✓ Revisar, analizar y aprobar los proyectos de seguridad de la información.
- ✓ Aprobar las modificaciones o nuevas políticas de seguridad de la información que se quieran implementar.
- ✓ Realizar análisis de riesgos a los sistemas de información que se manejan.
- ✓ Mantenerse actualizado en nuevas amenazas y vulnerabilidades existentes

ROLES: FUNCIONES Y RESPONSABILIDADES

A continuación se enumeran los roles que intervienen en el Comité de Seguridad de la Información del Área de Contabilidad.

Coordinador del Comité de Seguridad de la Información. Será el responsable de coordinar las acciones del Comité así como de impulsar la implementación y cumplimiento de la presente Política. Este rol recae sobre el Gerente de la E.S.E Hospital Local de Rio de Oro Cesar.

Responsable de Sistemas de Información.

Cumplirá funciones relativas a la seguridad del sistema de información (módulos – sistema contable TNS) del Área de contabilidad, lo cual incluye determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios usados en ésta. Este rol es desempeñado por el Ingeniero de Sistemas.

Responsable de los procesos contables:

Garantizar que de acuerdo al presupuesto para la ESE en las vigencias anuales, quede bien repartido entre los rubros presupuestales asignados en la institución, organiza los estados financieros de la E.S.E y garantiza los estados de los resultados financieros. Este rol es desempeñado por el Jefe del Área de contabilidad.

Responsable del Área de Recursos Humanos.

Pertenece al Comité de Seguridad de la Información y cumplirá la función de implicar a todo el personal del Área de contabilidad de la E.S.E en el conocimiento y cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan, así como de los cambios que en aquellas se produzcan. Igualmente, se responsabilizará de la implementación de los compromisos de confidencialidad que deban suscribir los empleados y de la capacitación continua de los mismos en materia de seguridad. Este rol es desempeñado por el Jefe de Recursos Humanos.

GESTIÓN DE ACTIVOS

Cada área, bajo supervisión del Comité de Seguridad de la Información debe elaborar y mantener un inventario de los activos de información que poseen, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

Controles:

- Se identificarán los activos importantes asociados al sistema contable TNS, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.
- El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 2 meses.
- Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.
- Se definirán procedimientos para el rotulado y manejo de información, de acuerdo al esquema de clasificación definido. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información: Copia, Almacenamiento, Transmisión por (correo, fax, correo electrónico), Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, entre otros).

CAPITULO II

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Orientadas a reducir los riesgos de error humano, comisión de ilícitos contra el Área de contabilidad de la E.S.E uso inadecuado de instalaciones, el Comité de Seguridad documentará las funciones de seguridad de los empleados y las Responsabilidades con respecto a la seguridad de la información.

Controles:

- El Comité de Seguridad desarrollará planes de capacitación de Seguridad de la Información, los cuales se realizarán periódicamente, mínimo una capacitación por semestre.

- Cuando un empleado se retire del Área de contabilidad, el Ingeniero de Sistemas, eliminará el usuario correspondiente a dicho empleado y debe hacer entrega del inventario de activos a su cargo.

- Como parte de sus términos y condiciones iniciales de empleo, los empleados firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información del área de contabilidad de la E.S.E.

- Todos los empleados del Área de contabilidad y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la misma, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimiento.

- Los empleados del Área de contabilidad, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Ingeniero de Sistemas.

SEGURIDAD FÍSICA Y DEL ENTORNO

Para el acceso a los sitios y áreas restringidas al Área de contabilidad de la E.S.E Hospital local de Rio de Oro Cesar, debe notificarse para la autorización correspondiente, y así proteger la información y los bienes informáticos, muebles e inmuebles y elementos hospitalarios.

Controles:

- La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas al Área de contabilidad.

- Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Jefe del Área de contabilidad, a fin de permitir el acceso sólo al personal autorizado.

- Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad.

- Para incrementar la seguridad de las áreas protegidas, se establecerán controles y lineamientos adicionales, para el personal que trabaja en el Área de contabilidad, así como para las actividades de terceros que tengan lugar allí.

- El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.

- El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo.

- El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño.

- Disponer de pólizas de protección de equipos actualizadas.

- El Comité de Seguridad, establecerá un plan de mantenimiento preventivo para los equipos y velará por el cumplimiento del mismo.

- El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la E.S.E Hospital Local de Rio de Oro Cesar será autorizado por el responsable patrimonial. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el Jefe del Área de contabilidad.

- La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento; medios de almacenamiento conteniendo material sensible.

- Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

- El equipamiento, la información y el software no serán retirados del Área de contabilidad sin autorización formal. Se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la E.S.E.

GESTIÓN DE COMUNICACIONES Y OPERACIONES

Los usuarios y funcionarios deben proteger la información utilizada en la infraestructura tecnológica del Área de contabilidad. De igual forma, deberán proteger la información reservada o confidencial que por necesidades de la empresa deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna a otras dependencias o redes externas como internet.

Controles:

- Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Ingeniero de Sistemas.

- El Ingeniero de Sistemas controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan.

- Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.

- Se contemplará la separación de la gestión o ejecución de tareas o áreas de responsabilidad, en la medida de que la misma reduzca el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.

- Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

- El Jefe del Área de contabilidad o su delegado, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados.

- El Jefe del Área de contabilidad y el Ingeniero de Sistemas sugerirán criterios de aprobación de nuevos sistemas de información para el Área de contabilidad, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva.

- El Ingeniero de Sistemas o su delegado, instalará antivirus en equipos de procesamiento de información del Área de contabilidad para actualizaciones diarias.

- El Jefe del Área de contabilidad desarrollará y verificará el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones del Área de contabilidad, que permita tomar medidas correctivas.

- El Ingeniero de Sistemas monitoreará permanentemente el tráfico de la red para detectar actividades inusuales o detrimento en el desempeño de la red.

- La E.S.E contará con un servidor en paralelo, el cual permitirá la continuidad de las operaciones, en caso de falla del servidor principal.

- El Comité de Seguridad de la Información garantizará la comunicación del Área de contabilidad con las demás Áreas mediante la existencia de líneas de back-up.

- El Jefe del Área de contabilidad, elaborará copias de seguridad diarias al sistema contable (TNS) y las guardará en sitios bajo llave. Es recomendable que las copias de seguridad se almacenen también en un lugar externo a la E.S.E para prevenir pérdida de datos en el caso de destrucción de la misma.

- El Jefe del Área de contabilidad o su delegado revisará semanalmente las copias de seguridad y llevará un registro de dicho procedimiento.

- Todo equipo de TI debe ser revisado, registrado y aprobado por el Ingeniero de Sistemas antes de conectarse a cualquier nodo de la red de comunicaciones, así mismo, desconectará aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

- No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor, en especial la ley 23 de 1982 y su modificación, la ley 44 de 1993 y la Decisión 351 de 1993. Ver la normatividad en la página:www.cecolda.org.co/index.php/derecho-de-autor/normas-y-jurisprudencia/normas-nacionales

- Las instalaciones de software deben ser aprobadas por el Ingeniero de Sistemas y en el caso de encontrarse software ilegal en el Área de contabilidad, será reportado como incidente de seguridad y posteriormente investigado.

- El Jefe del Área de contabilidad, con la asistencia del Ingeniero de Sistemas, implementará procedimientos para la administración de medios informáticos removibles, USB, CD´s, DVD e informes impresos y la eliminación segura de los mismos.

- Se tomarán recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada.

- Se implementarán normas, procedimientos y controles para proteger el intercambio de información a través de medios de comunicaciones de voz, fax y vídeo.

- El Comité de Seguridad Informática garantizará la protección contra la piratería y robo de información.

CONTROL DE ACCESO

En un sistema informático resulta de vital importancia, restringir los accesos y garantizar la adecuada utilización de los recursos informáticos.
Cada usuario y funcionario son responsables de los mecanismos de control de acceso que le sean proporcionados.

Controles:

- Corresponde al Ingeniero de Sistemas elaborar, mantener y publicar los documentos de servicios de red que ofrece la E.S.E. a todos los empleados y usuarios.

- El Ingeniero de Sistemas elaborará, mantendrá y publicará los procedimientos de administración de cuentas de usuario para el uso de servicios de la red.

- El Jefe de Recursos Humanos deberá comunicar al Ingeniero de Sistemas la relación de funcionarios públicos que hayan ingresado a laborar y de los que han dejado de hacerlo, para la activación o desactivación de los usuarios del sistema contable TNS respectivas.

- El Ingeniero de Sistemas definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso al Sistema contable TNS; se limitará y controlará la asignación y uso de privilegios.

- El Ingeniero de Sistemas o su delegado, configurará alertas de seguridad que permitan reaccionar de forma urgente ante determinados tipos de ataque e intentos de intrusión.

- Las contraseñas serán cambiadas periódicamente y suministradas al Ingeniero de Sistemas, cada vez que se haga el cambio.

- Los empleados del Área de contabilidad deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

- El Ingeniero de Sistemas, conjuntamente con el Jefe del Área de contabilidad, realizarán una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

- El Ingeniero de Sistemas debe coordinar con el Jefe de Recursos Humanos las tareas de concientización a todos los usuarios y contratistas del Área de contabilidad, acerca de los

requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

- Se podrán implementar controles para limitar la capacidad de conexión de los usuarios, de acuerdo a las políticas que se establecen a tal efecto.

- El Ingeniero de Sistemas junto con el Jefe del Área de contabilidad realizarán una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

- Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad. Los registros de auditoría deberán incluir la identificación del usuario, la fecha y hora de inicio y terminación, la identidad o ubicación de la terminal, un registro de intentos exitosos y fallidos de acceso al sistema y un registro de intentos exitosos y fallidos de acceso a datos y otros recursos.

- Se desarrollarán procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los empleados del Área de contabilidad sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.

- El proceso de autenticación al Sistema contable TNS, accedida debe ser de máximo tres intentos para una autenticación satisfactoria, después de éste número de intentos, se deshabilitará el ingreso de usuario.

- El acceso a los recursos de TI institucionales deben estar restringidos según los perfiles de usuario definidos por el Comité de Seguridad de la Información.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y Software de Base de Datos que integren el Área de contabilidad deben tener inmersos controles de seguridad de la información.

Controles:

- Las empresas con las cuales se realicen adquisiciones de software, deben tener mínimo certificación CMMI2.

- Las aplicaciones contarán con el Log de Auditoría, en el cual quedará registrado el usuario, la fecha, hora, módulo y opción a la que ingresó, facilitando al Ingeniero de Sistemas, la revisión de incidentes en el manejo de las aplicaciones.

- Se debe llevar una Bitácora con el control de cambios de las aplicaciones, indicando la fecha, hora, aplicación a la que se realizó el cambio, la causa, los cambios realizados y la persona que lo realizó.

- Incorporar seguridad al Sistema contable TNS y a las mejoras o actualizaciones que se les incorporen.

- Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo: Comprobaciones de la razonabilidad para probar si los datos de salida son plausibles; control de conciliación de cuentas para asegurar el procesamiento de todos los datos, provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información; procedimientos para responder a las pruebas de validación de salidas, definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

- Se garantizará que las actividades de soporte al Sistema contable TNS se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo.

- Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Una adecuada gestión de incidentes le permitirá al Área de contabilidad: responder a los incidentes de manera sistemática, eficiente y rápida; volver a la normalidad en poco tiempo, perder muy poca información; realizar continuamente mejoras en la gestión y tratamiento de incidentes; generar un Base de conocimientos sobre Incidentes; evitar en lo posible, incidentes repetitivos.

- El Ingeniero de Sistemas ante una incidencia, debe comunicarlo al Comité de Seguridad de la Información y diligenciará un formato donde quede consignados los datos de reporte del incidente y de la persona que reportó:

Reportes de Incidencias de seguridad informática.

REPORTE DE INCIDENTES
Datos del reporte de incidencia • Número • Fecha • Hora • Descripción del incidente • Efectos Producidos • Responsable del activo afectado • Causas del incidente (se diligencia, una vez se recupere la normalidad del proceso afectado)
Datos del reportante: • Nombre • Cargo • Dependencia • Correo

- Todos los empleados del Área de contabilidad, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.

- Una vez verificada la incidencia, el Ingeniero de Sistemas recolectará la información que le permitirá determinar el alcance del incidente, qué redes y que sistemas y aplicaciones fueron afectados, y que fue lo que generó el incidente, como ocurrió o está ocurriendo, también nos permite saber que originó el hecho, cómo ocurrió y las herramientas utilizadas, qué vulnerabilidades fueron explotadas y el impacto negativo que pueda tener sobre la E.S.E.

Para determinar el alcance, el Ingeniero de Sistemas puede hacerse las siguientes preguntas:

- ¿Cuántos equipos fueron comprometidos?
- ¿Cuántas redes se vieron envueltas?
- Hasta qué punto de la red logró penetrar el atacante?
- ¿Qué nivel de privilegio logró el atacante?
- ¿Qué es lo que está en riesgo?
- ¿Cómo impacta en las actividades de la E.S.E y en particular el Área de contabilidad?
- ¿Se encuentran en riesgo aplicaciones críticas?
- ¿Cuán conocida es la vulnerabilidad explotada por el atacante?
- ¿Hay otros equipos con la misma vulnerabilidad?

- Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información.

- Determinado el alcance del incidente de seguridad, el Ingeniero de Sistemas procederá a la contención, respuesta y puesta en marcha de las operaciones afectadas por el incidente.

La **contención,** evitará que el incidente siga produciendo daños. La **erradicación** eliminará la causa del incidente y todo rastro de los daños y la **recuperación**, consiste en volver el entorno afectado a su estado original.

Para llevar a cabo estas acciones, se tendrán que contar con estrategias que permitan realizar las operaciones de manera organizada, rápida y efectiva.

Para contar con una buena estrategia tengamos en cuenta estos agentes:

- Daño potencial de recursos a causa del incidente
- Necesidad de preservación de evidencia
- Tiempo y recursos necesarios para poner en práctica la estrategia
- Efectividad de la estrategia total o parcialmente
- Duración de las medidas a tomar
- Criticidad de los sistemas afectados
- Características de los posibles atacantes
- Si el incidente es de conocimiento público
- Pérdida económica
- Posibles implicancias legales
- Relación costo-beneficio de la estrategia
- Experiencias anteriores

- El Ingeniero de Sistemas, una vez neutralizado el incidente, procederá a investigar las causas de dicho incidente. Las causas se registrarán en el formato de reporte de incidentes.

La recolección de información cuando se investigan las causas debe respetar los siguientes puntos:

- **AUTENTICIDAD**: Quien haya recolectado la evidencia debe poder probar que es auténtica.

- **CADENA DE CUSTODIA**: Registro detallado del tratamiento de la evidencia, incluyendo quiénes, cómo y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma.

- **VALIDACION**: Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.

a. CUMPLIMIENTO

Todo uso y seguimiento de la seguridad de la información en el Área de contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar debe estar de acuerdo a las normas así como a la legislación nacional en la materia, incluido, pero no restringido a:

Constitución Política de Colombia: **Artículo. 61**.- El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley.
Ley 23 de 1982 Establece los derechos de autor.
Ley 1266 de 2008 (Habeas_Data)
Ley 1273 Delitos Informáticos
Ley 1581 Protección_Datos_Personales
Ley 488 de 1998 Se elimina el ajuste integral por inflación fiscal para los inventarios, ingresos, costos y gastos. Por expresa disposición del artículo 14 de la mencionada ley, estos cambios tienen efectos contables.
Normas técnicas generales de la contabilidad
Plan único de cuentas
Decreto 2193 aplicativo SIHO
Reportes y normas de supersalud
Normas de auditoría generalmente aceptadas NAGA
Decreto 2193 del MDPS
ISO 27002: Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable.

CAPÍTULO III

GLOSARIO

AMENAZA: Evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo a la organización.

BITÁCORA: Libro donde se registran las observaciones de un evento.

CONTRASEÑA: Conjunto de caracteres que permite el ingreso a un recurso informático.

CORTAFUEGOS: Parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

INCIDENTE DE SEGURIDAD: Es cualquier evento que pueda o pueda tener como resultado la interrupción de los servicios suministrados por un sistema informático y/o posibles pérdidas físicas, de activos o financieras. Es decir, se considera que un incidente es la materialización de una amenaza.

LOG DE AUDITORÍA: Término usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para una aplicación.

IMPACTO: Daño potencial sobre un sistema cuando una amenaza se presenta.

PLAN DE CONTINUIDAD DEL NEGOCIO: Estrategia planificada constituida por: un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación encaminada a conseguir una restauración progresiva y ágil de los servicios de negocio afectados por una paralización total o parcial de la capacidad operativa de la empresa.

RIESGO: Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización.

SERVIDOR: Computadora que ejecuta un programa que realiza alguna tarea en beneficio de otras aplicaciones llamadas clientes.

SISTEMA DE INFORMACIÓN: Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

TI: Tecnología de la Información y Comunicaciones.

VULNERABILIDAD: Cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir pérdidas para la organización.

HISTÓRICO DE REVISIONES, ACTUALIZACIONES Y APROBACIONES

Cada año la Política de Seguridad debe ser revisada y retroalimentada en los aspectos que sean necesarios mínimo cada año, y los cambios serán documentados en un Registro de Cambios de la Política de Seguridad Informática, se harán las modificaciones respectivas en el documento y posteriormente, se promulgará mediante Resolución.

El Comité de Seguridad de la Información divulgará la Política de Seguridad Informática a todos los departamentos de la E.S.E.

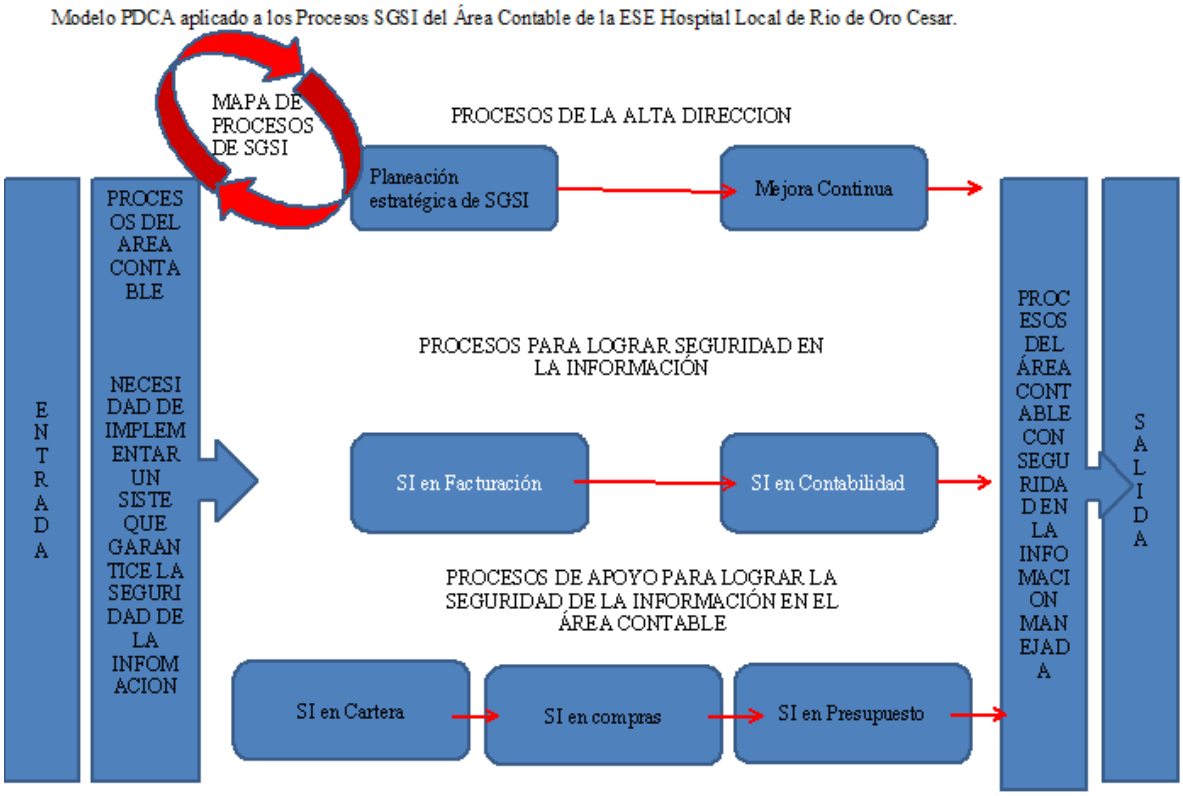
Registro de cambios de la política de seguridad de la información					
Año	**Aspectos a modificar**	**Control actual**	**Control modificado**	**Persona que realiza la modificación**	**Cargo**

COMUNÍQUESE Y CÚMPLASE

Dado en la ciudad de Ocaña, a los 2 días del mes de diciembre de 2013.

LORENA SEPULVEDA
Jefe del Área de contabilidad
E.S.E Hospital Local de Rio de Oro Cesar

7. MAPA DE PROCESOS DE SGSI EN EL ÁREA CONTABLE DE LA ESE HOSPITAL LOCAL DE RIO DE ORO CESAR.



8. CARACTERIZACIÓN DE PROCESOS DE SGSI DEL ÁREA CONTABLE DE LA ESE HOSPITAL LOCAL DE RIO DE ORO CESAR.

	CARACTERIZACIÓN DEL PROCESO DE **SEGUIMIENTO Y MEJORA** FICHA TÉCNICA Sistema de Gestión de Seguridad de la Información	VERSIÓN	FECHA	PAGINA		
		1	12 /11/2013	1	DE	2

MANUAL DE SEGURIDAD DE LA INFOMACION

PLAN DE SEGUIMIENTO DE LOS INDICADORES DE LOS OBJETIVOS DEL SGSI

PROCESO DE SEGUIMIENTO Y MEJORA

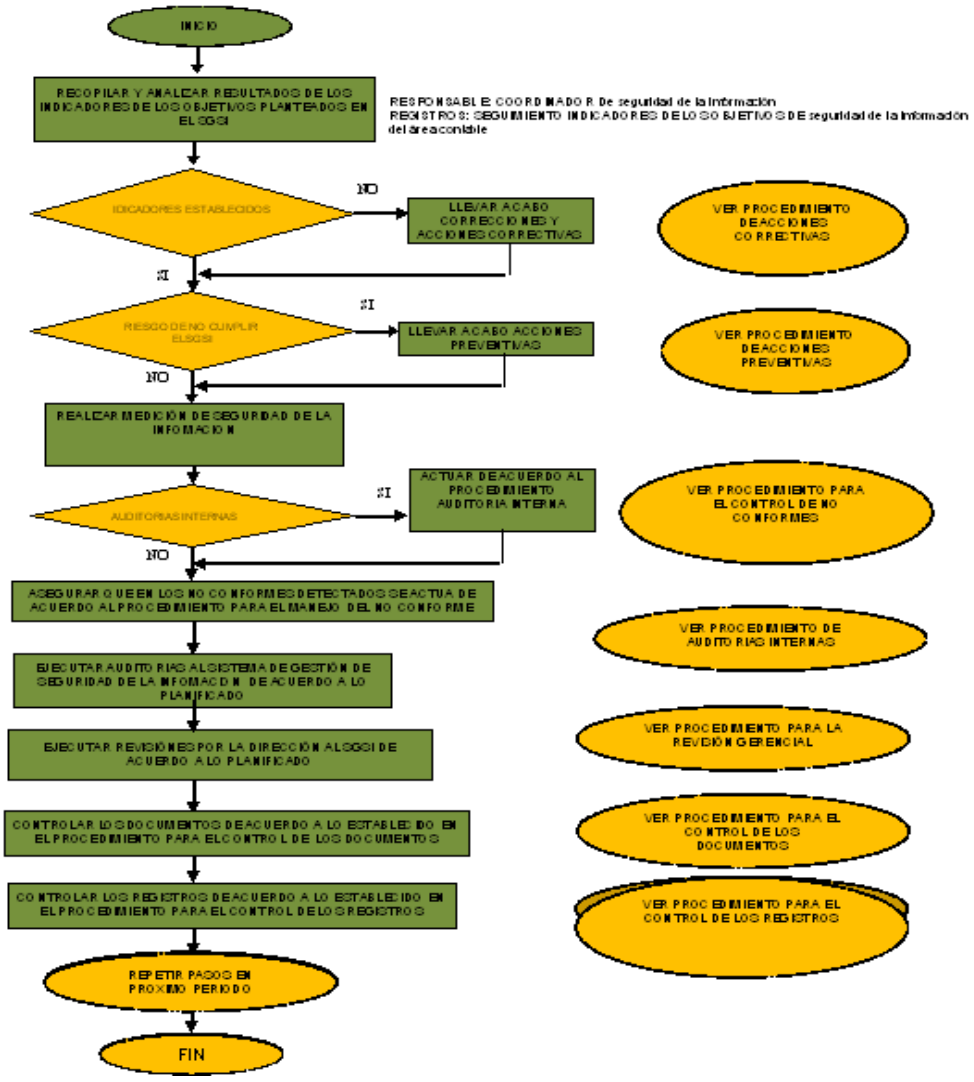
SEGUIMIENTOS A INDICADORES, ANÁLISIS DE INDICADORES, AUDITORÍAS AL SGSI, REVISIONES GERENCIALES DE TI

IA

OBJETIVO	EFECTUAR LAS ACTIVIDADES DE SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y MEJORA NECESARIAS PARA ASEGURAR LA CONFORMIDAD DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA CONTABLE DE LA ESE HOSPITAL LOCAL DE RIO DE ORO CESAR
ALCANCE	LAS ACTIVIDADES RELATIVAS AL SEGUIMIENTO, LA MEDICIÓN, EL ANÁLISIS Y LA MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN LOS PROCESOS
RESPONSABLE	CORDINADOR DE SEGURIDAD DE LA INFOMACION
GRUPO DE TRABAJO	COORDINADOR DE SEGURIDAD DE LA INFOMACION
PROVEEDOR INTERNO	PROCESOS DEL ÁREA CONTABLE
CLIENTE INTERNO	PROCESOS DEL ÁREA CONTABLE
PROCESOS DE SOPORTE	PLANEACIÓN ESTRATÉGICA DE SI
DOCUMENTOS	• PROCEDIMIENTO DE ACCIONES CORRECTIVAS AL SGSI DEL ÁREA CONTABLE • PROCEDIMIENTO DE ACCIONES PREVENTIVAS AL SGSI DEL ÁREA CONTABLE • PROCEDIMIENTO PARA EL CONTROL DE NO CONFORME AL SGSI DEL ÁREA CONTABLE • PROCEDIMIENTO DE ACCIONES DE MEJORAS AL SGSI DEL ÁREA CONTABLE • PROCEDIMIENTO DE ANÁLISIS DE DATOS AL SGSI DEL ÁREA CONTABLE • PROCEDIMIENTO DE AUDITORIAS INTERNAS AL SGSI DEL ÁREA CONTABLE • PROCEDIMIENTO PARA EL CONTROL DE LOS DOCUMENTOS AL SGSI DEL ÁREA CONTABLE • PROCEDIMIENTO PARA EL CONTROL DE LOS REGISTROS AL SGSI DEL ÁREA CONTABLE
Ítems de la norma 27001 – 2005 relacionados	**b. A.5.1 – A.5.1.1 – A.5.1.2 – A.6.1 – A.6.2 – A.7.1 – A.7.2 – A.8.1 – A.8.2 – A.8.3 – A.7.1 – A.9.2 - A.10.1 – A.10.3 – A.10.5 – A.10.8 – A.10.9 – A.10.10 – A.10.11 – A.11.1 – A.11.2 – A.11.3 – A.11.4 – A.11.5 - A.11.6 – A.12.1 – A.12.3 – A.12.4 – A.12.6 - A.12.1 – A.13.2 – A.14.1 - A.15.1 – A.15.2 - A.14.3 -**
RECURSOS	COMPUTADORES, ELEMENTOS DE OFICINA, ELEMENTOS DE COMUNICACIÓN,

	ELEMENTOS INFORMACION
INDICADOR	- GRADO DE IMPLEMENTACIÓN DEL SGSI DEL ÁREA CONTABLE DE LA ESE OLRC - EFICACIA DE LAS ACCIONES CORRECTIVAS Y PREVENTIVAS - EFICACIA DE LAS AUDITORÍAS INTERNAS
META	- ≥ 80 % - ≥ 70 % - ≥ 70 %

HOSPITAL LOCAL ESE RIO DE ORO-CESAR	CARACTERIZACIÓN DEL PROCESO DE **SEGUIMIENTO Y MEJORA** FLUJOGRAMA	VERSIÓN	FECHA	PAGINA		
		1	12/11/2013	2	DE	2

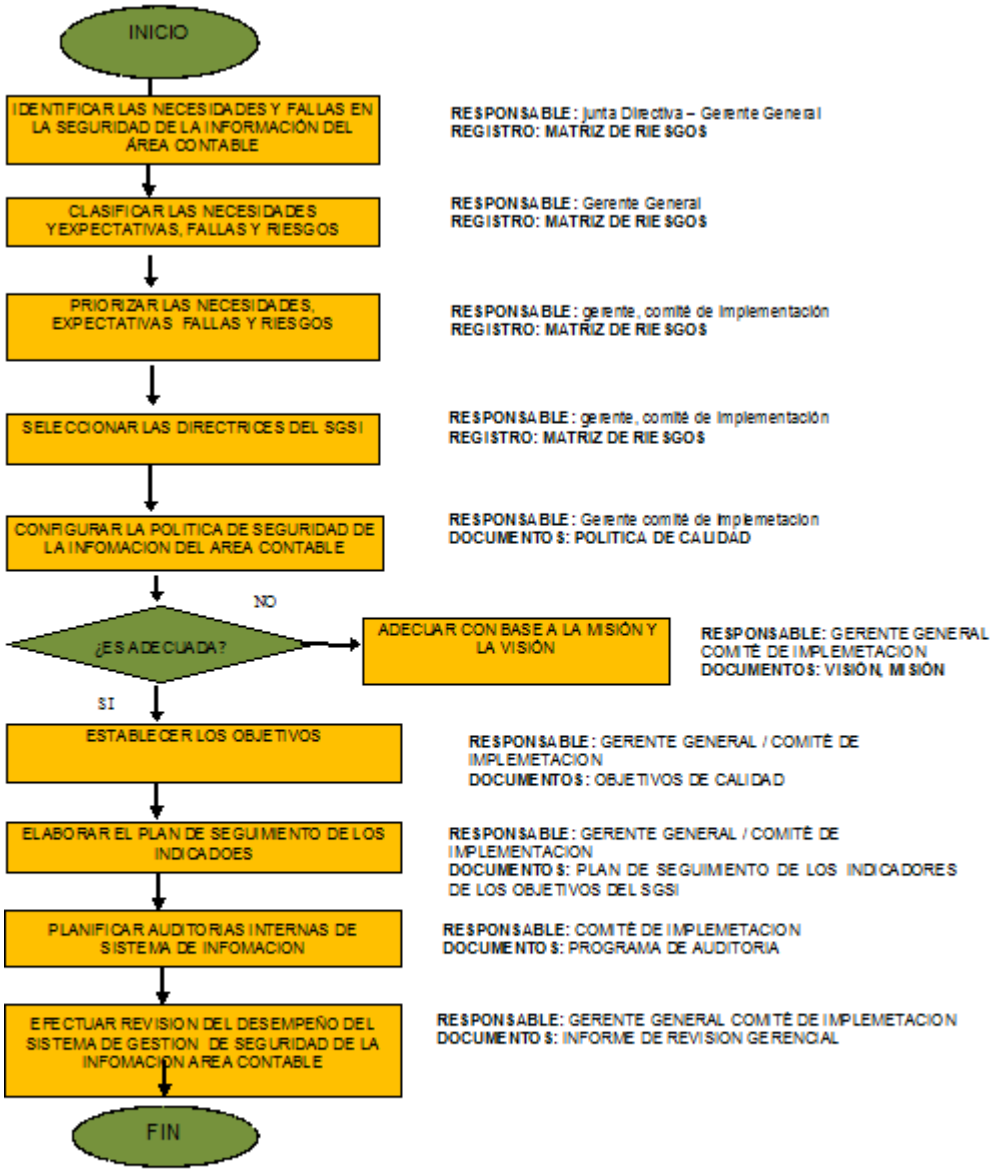


	CARACTERIZACIÓN DEL PROCESO DE **planeación estratégica del SGSI** FICHA TÉCNICA Sistema de Gestión de Seguridad de la Información	VERSIÓN	FECHA	PAGINA		
		1	12 /11/2013	1	DE	2

OBJETIVO	PLANIFICAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION CON EL FIN DE ESTABLECER LA POLÍTICA DE SEGURIDAD DE LA INFOMACION DEL AREA CONTABLE, LOS OBJETIVOS DE SEGURIDAD DE LA INFOMACION DEL AREA CONTABLE, CUMPLIR CON LOS REQUISITOS DE LA NORMA ISO 27001 Y 27002 – 2005 Y GARANTIZAR LA EFICACIA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION DEL AREA CONTABLE DE LA ESE HLRC
ALCANCE	LAS ACTIVIDADES RELATIVAS A LA PLANEACIÓN ADMINISTRATIVA Y DE SISTEMAS DE INOFMACION DEL AREA CONTABLE DE ESE
RESPONSABLE	GERENTE Y JUNTA DIRECTIVA DE LA ESE
GRUPO DE TRABAJO	COORDINADOR DEL SGSI, COMITÉ DE IMPLEMETACION
PROVEEDOR INTERNO	TODOS LOS PROCESOS DEL AREA CO NTABLE
Ítems de la norma 27001 – 2005 relacionados	MODELO PDCA APLICADO A LOS PROCESOS DEL SGSI A.5 -. A.6 – A.7 – A.8 – A.9 – A.10 – A.11 – A.12 Se excluye A.12.3 – A.13 – A.14 se excluye a.14.1 – A.15
CLIENTE INTERNO	TODOS LOS PROCESOS DEL ARA CONTAB LE
PROCESOS DE SOPORTE	SEGUIMIENTO Y MEJORA
DOCUMENTOS	- MISIÓN, VISIÓN, POLÍTICA DE SEGURIDAD DE LA INFOMACION DEL AREA CONTABLE, OBJETIVOS, MAPA DE PROCESOS AREA CONTABLE. - PLAN DE SEGUIMIENTO DE LOS INDICADORES DE LOS OBJETIVOS DE LOS PROCESOS - MANUAL DE SEGURDIAD DE LA INFOMACION DEL AREA CONTABLE - PROGRAMA DE AUDITORIA INTERNA DEL SEGURIDAD DE INFOMACION DEL AREA CONTABLE - PROCEDIMIENTO DE PLANEACIÓN ESTRATÉGICA DE SGSI AREA CONTABL. - PROCEDIMIENTO DE REVISIÓN GERENCIAL
REGISTROS	**i. INFORME DE REVISIÓN**

	GERENCIAL
RECURSOS	COMPUTADORES, ELEMENTOS DE OFICINA, ELEMENTOS DE COMUNICACIÓN
INDICADOR	- EFICACIA EN EL CUMPLIMIENTO DE LOS INDICADORES - PORCENTAJE DE PERDIDA DE INFOMACION AREA CONTABLE - PRODUCTIVIDAD FINANCIERA DE LA ESE
META	- ≥ 70 % - ≥ 10% - ≥ 20% AUMENTO

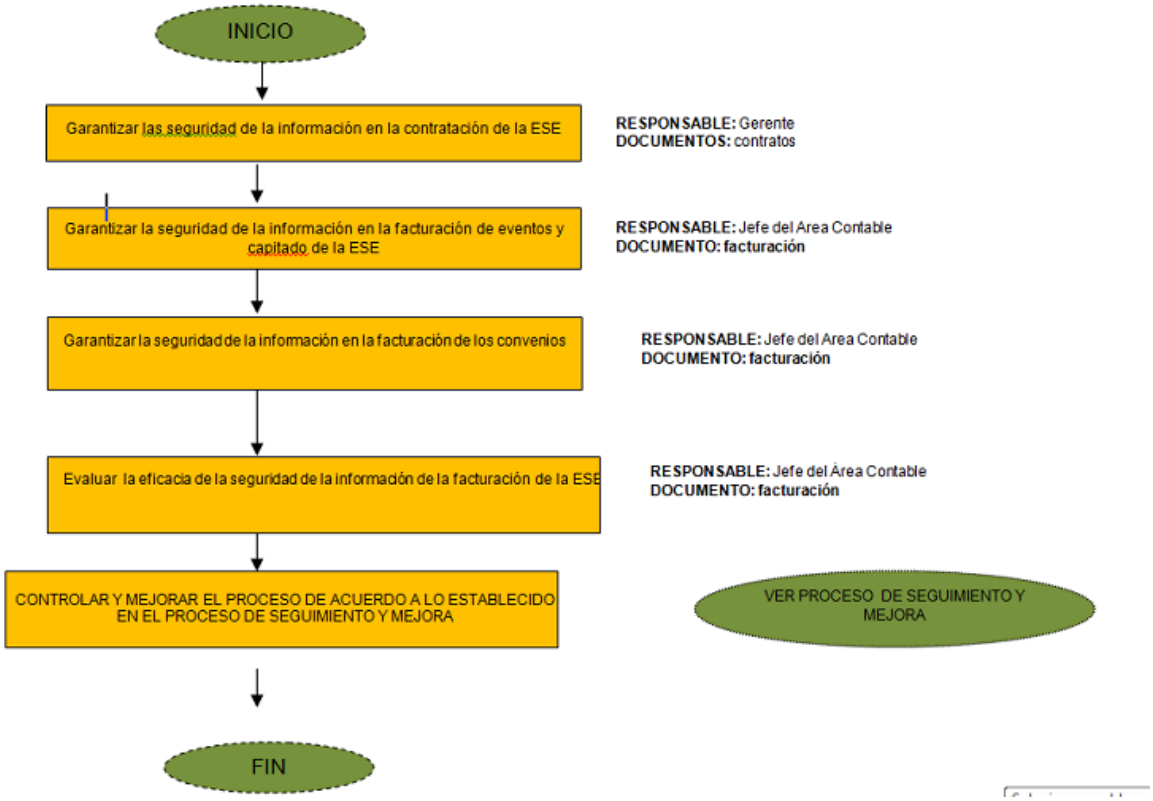
	CARACTERIZACIÓN DEL PROCESO de planeación estratégica del SGSI Área Contable FLUJOGRAMA	VERSIÓN	FECHA	PAGINA		
		1	12/11/2013	2	DE	2



	CARACTERIZACIÓN DEL PROCESO DE **Facturación** FICHA TÉCNICA Sistema de Gestión de Seguridad de la Información	VERSIÓN	FECHA	PAGINA		
		1	12 /11/2013	1	DE	2

OBJETIVO	GARANTIZAR QUE LA FACTURACIÓN DE LA ESE MANTENGA LA SEGURIDAD EN LA INFORMACIÓN ESPERADA UTILIZANDO LOS CONTROLES DE LA 27001. 2005 Y MINIMIZANDO RIESGOS
ALCANCE	LAS ACTIVIDADES RELATIVAS A LA FACTURACIÓN DE LA ESE
RESPONSABLE	JEFE DEL ÁREA CONTABLE DE LA ESE
GRUPO DE TRABAJO	JEFE DEL AREA CONTABLE – FACTURADORES – AUDITORES
PROVEEDOR INTERNO	CONTRATACION
Ítems de la norma 27001 – 2005 relacionados	MODELO PDCA APLICADO A LOS PROCESOS DEL SGSI A.5 -. A.6 – A.7 – A.8 – A.9 – A.10 – A.11 – A.12 Se excluye A.12.3 – A.13 – A.14 se excluye a.14.1 – A.15
CLIENTE INTERNO	CONTABILIDAD
PROCESOS DE SOPORTE	SEGUIMIENTO Y MEJORA
DOCUMENTOS	- RESGISTROS DE FACTURACIONCON SEGURIDAD EN LA INFOMACION
REGISTROS	**ii. FACTURAS**
RECURSOS	COMPUTADORES, ELEMENTOS DE OFICINA, ELEMENTOS DE COMUNICACIÓN, ELEMETOS DE INFOMACION
INDICADOR	- FACTURACION CON SEGURIDAD EN LA INFOMACION
META	- ≥ 80 %

	CARACTERIZACIÓN DEL PROCESO de Facturación del SGSI Área Contable FLUJOGRAMA	VERSIÓN	FECHA	PAGINA		
		1	12/11/2013	2	DE	2

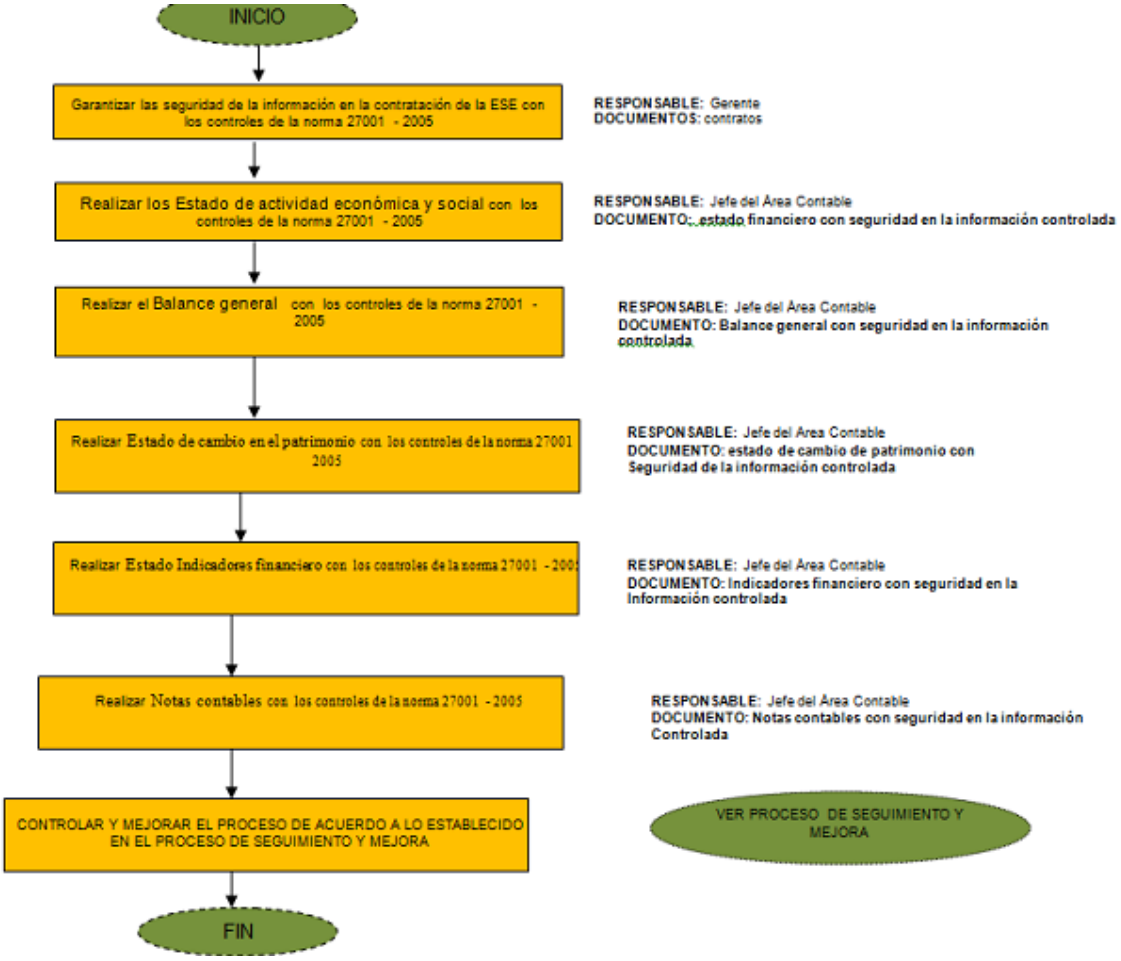


	CARACTERIZACIÓN DEL PROCESO DE **Contabilidad** FICHA TÉCNICA Sistema de Gestión de Seguridad de la Información	VERSIÓN	FECHA	PAGINA		
		1	12 /11/2013	1	DE	2

Contabilidad si n seguridad en la información → **PROCESO DE CONTABILIDAD** → Contabilidad con seguridad en la información manejada

OBJETIVO	GARANTIZAR QUE LA CONTABILIDADDE LA ESE MANTENGA LA SEGURIDAD EN LA INFORMACIÓN ESPERADA UTILIZANDO LOS CONTROLES DE LA 27001. 2005 Y MINIMIZANDO RIESGOS
ALCANCE	LAS ACTIVIDADES RELATIVAS A LA CONTABILIDAD DE LA ESE
RESPONSABLE	JEFE DEL ÁREA CONTABLE DE LA ESE
GRUPO DE TRABAJO	JEFE DEL AREA CONTABLE – CONTADOR- AUXILIAR CONTABLE
PROVEEDOR INTERNO	FACTURACION
Ítems de la norma 27001 – 2005 relacionados	MODELO PDCA APLICADO A LOS PROCESOS DEL SGSI A.5 -. A.6 – A.7 – A.8 – A.9 – A.10 – A.11 – A.12 Se excluye A.12.3 – A.13 – A.14 se excluye a.14.1 – A.15
CLIENTE INTERNO	CARTERA – COMPRAS – ALMACEN
PROCESOS DE SOPORTE	SEGUIMIENTO Y MEJORA
DOCUMENTOS	- CONTABILDIAD CON LA SEGURIDAD DE LA INFORMACION MAJEFADA
REGISTROS	Estado de actividad económica y social con seguridad de la información manejada Balance general con seguridad de la información manejada Estado de cambio en el patrimonio con seguridad de la información manejada Indicadores financiero con seguridad de la información manejada Notas contables con seguridad de la información manejada **iii.**
RECURSOS	COMPUTADORES, ELEMENTOS DE OFICINA, ELEMENTOS DE COMUNICACIÓN, ELEMETOS DE INFOMACION
INDICADOR	- CONTABILIDAD CON SEGURIDAD EN LA INFOMACION
META	- ≥ 80 %

	CARACTERIZACIÓN DEL PROCESO de Contabilidad del SGSI Área Contable FLUJOGRAMA	VERSIÓN	FECHA	PAGINA		
		1	12/11/2013	2	DE	2



9. PROCEDIMIENTO PARA ACCIONES CORRECTIVAS

OBJETO: Mejorar la eficacia del Sistema de Gestión de Seguridad de la Información mediante la identificación e implementación de acciones correctivas que permitan eliminar las causas de no conformidades con el propósito que no vuelvan a ocurrir.

ALCANCE: Este procedimiento aplica para todas las no conformidades detectadas en el sistema de gestión de seguridad en la información del área contable de la ESE Hospital Local de Rio de Oro Cesar

DEFINICIONES:

No conformidad: Incumplimiento de un Control.

Acción Correctiva: Acción tomada para eliminar la causa de una no conformidad detectada u otra situación indeseable.

Corrección: Acción tomada para eliminar una no conformidad.

RESPONSABLES:

Coordinador de Seguridad de la Información: Es el encargado de verificar el cumplimiento de las tareas establecidas como acción correctiva y de verificar y garantizar que el cierre de la acción correctiva sea eficaz.

El responsable del área cotable y su grupo de trabajo: son los encargados de describir la no conformidad, establecer las causas, la acción correctiva, definir las tareas y de presentar al coordinador de seguridad de la infomacion el registro de las acciones correctivas identificadas.

CONTENIDO:

Revisar las No conformidades identificadas en la evaluación del desempeño del sistema de gestión de seguridad de la información (auditorías internas, revisión gerencial, oportunidades de mejora, retroalimentación de los sistemas de información , desempeño de los procesos, conformidad de la seguridad en la infomacion).

Realizar el análisis de las No Conformidades detectadas y determine si se hace necesario la adopción de una corrección o una acción correctiva.

En caso de ser necesario adoptar una acción correctiva, determine las causas de la no conformidad, utilizando herramientas de análisis tales como lluvia d ideas, diagrama causa-efecto y los tres porqués,

Con base a las causas de la no conformidad implemente las acciones necesarias para eliminar las causas de la no conformidad.

Documente en el registro de acciones correctivas los resultados de las acciones tomadas. Revise de acuerdo a la fecha de cierre de la acción correctiva si la acción ha sido apropiada a los efectos de la no conformidad encontrada.

DOCUMENTOS RELACIONADOS

Informe de auditorías internas de sistema de seguridad de la información del área contable
Informe de revisión gerencial.

Acta de análisis de indicadores de los objetivos del SGSI

Procedimiento de Análisis de datos.

REGISTROS:

Acciones correctivas.

ANEXOS:

No aplica

10. PROCEDIMIENTO PARA ACCIONES PREVENTIVAS

OBJETO: Mejorar la eficacia del Sistema de Gestión De Seguridad de la Información en el área contable mediante la identificación e implementación de acciones preventivas.

ALCANCE: Aplica a los procesos del área contable descritos en el mapa de procesos
DEFINICIONES:

No Conformidad: Incumplimiento de un requisito

Acción Preventiva: Acción tomada para eliminar la causa de una no conformidad potencial u otra situación potencialmente no deseable.
Reproceso: Acción tomada sobre un producto no conforme para que cumpla con los requisitos.

RESPONSABLES:

El Coordinador de Seguridad de la Infomacion: Es el encargado de verificar el cumplimiento de las tareas establecidas como acción preventiva y de verificar y garantizar que el cierre de la acción preventiva sea eficaz.

El responsable del área contable y su grupo de trabajo: son los encargados de describir la no conformidad, establecer las causas, la acción preventiva, definir las tareas y de presentar al coordinador de seguridad de la información el registro de las acciones preventivas identificadas.

CONTENIDO:

- Identificar y registrar las No conformidades potenciales de acuerdo al procedimiento del área contable de la ESE Hospital Local de Rio de Oro Cesar de las Acciones Preventivas.
- Realizar el análisis de las No Conformidades potenciales para identificar las causas básicas.
- Definir las acciones preventivas que permitan eliminar las causas de las no conformidades potenciales utilizando como herramienta de análisis de modo y efectos de falla (AMEF) descrito en el procedimiento de análisis de datos, como técnica para identificar las causas potenciales.
- Con base a las causas de la no conformidad potencial implemente las acciones necesarias para eliminar las causas.
- Documente en el control de acciones preventivas los resultados de las acciones tomadas.
- Revise de acuerdo a la fecha de cierre de la acción preventiva si la acción ha sido apropiada a los efectos de la no conformidad potencial encontrada.

DOCUMENTOS RELACIONADOS:

Procedimiento de Análisis de datos.

REGISTROS:

Acciones preventivas.

ANEXOS:

No aplica

11. PROCEDIMIENTO PARA AUDITORÍAS INTERNAS

OBJETO: Establecer un procedimiento que describa las actividades requeridas para determinar si el sistema de gestión de Seguridad de la Información del área contable de la ESE Hospital Local de Rio de Oro Cesar conforme con las disposiciones planificadas, con los requisitos de la Norma ISO 27001:2005 y si se ha implementado y se mantiene de manera eficaz.

ALCANCE: Este procedimiento aplica a las actividades relativas a la programación y realización de auditorias internas.

DEFINICIONES:

Auditoria: Proceso sistemático, independiente y documentado para obtener evidencia de la auditoria y evaluar de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de auditoria.

Auditoria Externa: Son denominadas auditorias de segunda y tercera parte, las de segunda parte se llevan a cabo por parte de quienes tienen interés en la organización, y las de tercera parte son las realizadas por organizaciones independientes, las cuales proporcionan la certificación. Tienen una frecuencia de 3 años.

Auditorias Internas: Son las efectuadas por la ESE Hospital Local de Rio de Oro Cesar, con personal propio.

Auditoria De Seguimiento O Mantenimiento: Es aquella que se hace para verificar si se han cumplido las acciones correctivas encontradas en las auditorias de Certificación. Estas las desarrollará la entidad certificadora bajo los criterios de las normas ISO 27001 VERSION 2005, con una frecuencia semestral.

Auditor: Persona calificada para desempeñar auditorias del Sistema de Gestión de Seguridad de la Información con la norma ISO 27001: 2005.

Auditor Líder: Persona calificada para gerenciar y desempeñar auditorias al Sistema de Gestión de Seguridad de la Información y de la norma ISO 27001:2005, según el criterio de calificación de las mismas.

Evidencias De Auditoria: Registros, declaraciones de hechos o cualquier otra información que son pertinentes para los criterios de auditoria

Acción Correctiva: Acción de control reactiva tomada para eliminar la causa de una no conformidad real, sea mayor, menor u observación.

Acción Preventiva: Acción de control proactiva tomada para eliminar la causa de una no conformidad mayor, menor u observación potencial detectada.

No Conformidad: es cualquier desviación respecto a los controles de la normas, prácticas, procedimientos, reglamentos del desempeño del Sistema de Gestión de Seguridad de la Información.

No Conformidad Mayor: Son las desviaciones que comprometen la efectividad del sistema de gestión de Seguridad en la Información en el área contable generalmente dirigidas a incumplimiento generalizado en la compañía o ausencia de un procedimiento mandatorio de la norma ISO 27001: 2005.

No Conformidad Menor: Son incumplimientos aislados que no comprometen la efectividad del Sistema de gestión de Seguridad de la Información. La repetitividad sistemática de estos eventos podría constituir una NO CONFORMIDAD MAYOR.

Hallazgos De La Auditoria: resultado de la evaluación de la evidencia de la auditoria, recopilada frente a criterios de auditoria

RESPONSABLES:

Gerente de la ESE: Es el encargado de la revisión de los informes de las auditorias internas y de gestionar los planes de acciones correctivas de acuerdo a los hallazgos de la auditoria.

El Coordinador de Seguridad de la Infomacion : Es el encargado de la programación, planificación y realización de las auditorias internas del Sistema de Información del área contable conjuntamente con los auditores internos seleccionados.

Auditor Líder: Es el encargado de la programación, realización de las auditorias internas y realización y distribución del informe de auditoria

CONTENIDO:

Recomendaciones Generales:

- Los auditores no deben realizar auditorias a las actividades o procesos por los cuales son responsables directos, con el fin de no afectar la objetividad.
- La auditoria interna se realizará con una frecuencia mínima anual (un ciclo).
- Las Auditorias deben ser realizadas por auditores internos o externos, siempre y cuando cumplan con el nivel de competencias definido para los auditores internos de seguridad en la Información

Selección de los auditores: La organización ha establecido que las auditorias internas pueden ser realizadas por personal interno o externo, previo cumplimiento de los siguientes requisitos de competencias:

- ✓ Educación: Profesional en áreas administrativas y especialista en Auditoria de Sistemas.
- ✓ Formación: 16 horas en análisis e interpretación de la Norma ISO 27001:27002 de 2005 y 40 horas en técnicas de auditoria.
- ✓ Experiencia: mínima de 2 ciclos de auditorias internas.

Programa de auditoria: El coordinador de Seguridad de la Información, conjuntamente con el auditor líder, establecerá el programa de auditoria el cual mínimo debe contener: el objetivo, el alcance, los criterios de auditoria, la metodología, los procesos, fechas, horas para la realización de la auditoria y los auditores para cada proceso del área contable de la ESE

Desarrollo de La Auditoria: Para el desarrollo de la auditoria la organización ha establecido las siguientes fases:

Reunión de apertura: En esta reunión el auditor líder presenta al equipo auditor y solicita una presentación del equipo auditado. Seguidamente hace conocer el programa de auditoria y determina si existe alguna modificación en el programa, finalmente fija la hora tentativa de cierre.

Realización de la auditoria: El grupo auditor inicia la realización de la auditoria de acuerdo al programa para lo cual, conjuntamente con el auditado, establece la metodología (entrevista, observación y revisión de documentos) y da a conocer y explica los potenciales hallazgos (recomendaciones, observaciones y no conformidades). Finalmente realiza el cierre parcial de cada proceso auditado dando a conocer los hallazgos encontrados con el responsable da cada proceso.

Recopilación de los hallazgos y elaboración del informe: El auditor líder recopila y discute los hallazgos encontrados por el grupo auditor y elabora el informe final.

Reunión de cierre: El auditor líder presenta ante los auditados el informe fina de auditoria en el siguiente orden:

- ✓ Agradecimiento por la colaboración prestada
- ✓ Comunica las dificultades presentadas durante la auditoria
- ✓ Da a conocer las fortalezas de la organización
- ✓ Da a conocer los aspectos por mejorar
- ✓ Da a conocer los hallazgos de la auditoria del SGSI Área contable(no conformidades).
- ✓ Finalmente presenta las conclusiones de la auditoria y hace entrega del informe final al coordinador de Seguridad de la Información

DOCUMENTOS RELACIONADOS:

Norma ISO 27001:2005
Norma ISO 27002:2005
Norma ISO 19011.

Manual de Seguridad de la Información del Área contable
Manual de Procedimientos.

REGISTROS:

Informe de Auditorias.
Acción correctiva.

ANEXOS:

Programa de auditorías.

12. PROCEDIMIENTO PARA EL CONTROL DE DOCUMENTOS

OBJETO: Controlar los documentos del Sistema de Gestión de Seguridad de la Información del área contable de la ESE Hospital Local de Rio de Oro Cesar para asegurar que éstos se puedan entender y operar de manera efectiva, eficiente y en conformidad con los requisitos de las norma ISO 27001 versión 2005.

ALCANCE: Aplica a todos los documentos internos y externos, para el Sistema de gestión de Seguridad de la Información del área contable de la ESE Hospital Local de Rio de Oro Cesar

DEFINICIONES:

Información: Datos que posee significado.

Documento: Información y su medio de soporte.

Documento Externo: Todo documento que no es generado por el area contable de la ESE Hospital Local de Rio de Oro Cesar, pero necesario para la aplicación durante la ejecución contable de la ESE.

Copia Controlada: Son las copias de los procedimientos de trabajo que se suministran en reemplazo del documento original. Toda copia controlada debe tener un sello en la primera que diga "Copia Controlada"

Copia No Controlada: Son copias de documentos que se suministran con el único propósito de información de referencia y no deben usarse para otro fin distinto.

Documento Obsoleto: Es un documento que perdió su validez y no debe ser utilizado.
Procedimiento: Descripción de tareas.

Listado Maestro de Documentos: Registro en donde se relacionan todos los documentos críticos controlados del Sistema de Gestión de Seguridad de la Información en el área contable de la ESE Hospital Local de Rio de Oro Cesa

Listado Maestro de Registros: Registro en donde se relacionan todos los registros críticos controlados del Sistema de Gestión de Seguridad de la Información en el área contable de la ESE Hospital Local de Rio de Oro Cesar

RESPONSABLES:

Coordinador de Seguridad de la Información: Responsable por el control de documentos del Sistema de Gestión de Seguridad de la Información en el área contable de la ESE Hospital Local de Rio de Oro Cesar, en cuanto a la revisión, distribución, actualización y registro de los mismos en el Listado maestro de control de documentos.

Gerente: Encargado de la aprobación de los documentos del Sistema de Gestión de Seguridad de la Información en el área contable de la ESE Hospital Local de Rio de Oro Cesar.

Nota: Cada proceso es responsable por la elaboración de sus procedimientos.

CONTENIDO:

Los documentos controlados deben estar ubicados en un archivo en el disco duro y una copia magnética. Estos pueden ser consultados por toda la Organización pero solo el responsable del documento puede efectuar actualizaciones con las aprobaciones respectivas (Coordinador de Seguridad de la Información y Gerencia).

Adicionalmente podrán existir documentos en copias duras controladas.

Los documentos controlados serán revisados y actualizados cada año.

Los documentos controlados se elaborarán de acuerdo con el procedimiento para elaborar documentos.

Cuando se requiera hacer una modificación o revisión de un documento existente, éste deberá realizarse a través del Coordinador de seguridad e la informacion quien tomará la copia del disco duro o del medio magnético, realizará las modificaciones que se requieran y enviará el borrador modificado para aprobación del gerente. Los cambios en el documento serán señalados en el Listado Maestro de Documentos.

El coordinador de Seguridad del Información debe garantizar que las versiones pertinentes de los documentos aplicables se encuentren disponibles en cada proceso, haciendo entrega de los documentos y registros a los responsables de cada proceso, controlándolos en el Listado maestro de Documentos, con su firma de recibido.

Los documentos obsoletos se identifican un sello que diga “Documento Obsoleto” en caso de que se mantengan por cualquier circunstancia o se destruyen en caso de no ser necesario su mantenimiento.

Nota:

1. Todo documento que no posee el sello de copia controlada en la primera página se considera como copia no controlada.
2. Todo documento del SGSI debe ser legible y fácilmente identificable por medio del título y del tipo de documento. Su protección se dará en carpetas foliadas, con protectores de hojas e identificación adecuada, según su documento.

Para el control de los documentos externos se establece como mecanismo de control la identificación por medio de un sello que dice documento de origen externo copia

controlada. Además el gerente y el Coordinador de Seguridad de la infomacion deben revisar con una frecuencia semestral la vigencia de estos documentos, verificando en la red de las entidades competentes.

DOCUMENTOS RELACIONADOS:

Manual de Seguridad de la Información del área contable de la ESE
Manual de Procedimientos.

Procedimiento para la elaboración de documento.

REGISTROS:

Listado Maestro de Control de documentos.

ANEXOS: No aplica.

13. PROCEDIMIENTO DE CONTROL DE REGISTRO

OBJETO: Establecer la forma de identificar, almacenar, proteger, recuperar, definir el tiempo de retención y disposición de los registros que se requieran dentro del Sistema de Gestión de Seguridad de la Información en el Área contable de la ESE Hospital Local de Rio de Oro Cesar

ALCANCE: Aplica a todos los registros del SGSI del Área contable de la ESE Hospital Local de Rio de Oro Cesar

DEFINICIONES:

SGSI: Sistema de Gestión de Seguridad de la Información

Información: Datos que poseen significado.

Documento: Información y su medio de soporte.

Registro: Documento que presenta resultados obtenidos o proporciona evidencia de actividades desempeñadas y controles ejecutados.

RESPONSABLES:

Coordinador De Seguridad de la Información: Responsable de mantener actualizado este procedimiento.

El responsable del área contable y su grupo de trabajo: Responsable del diligenciamiento y almacenamiento de los respectivos registros de su proceso.

CONTENIDO: Los registros del Sistema de Gestión de seguridad de la infomacion deben cumplir con:

Identificación: Los registros se identifican, como mínimo, con la siguiente información:

Nombre del registro asociado a la actividad realizada.

Fecha de ejecución de la actividad.

Las columnas y filas de la información requerida.

Almacenamiento:

Los registros pueden ser guardados en medio electrónico o copia dura de acuerdo a los requerimientos de cada área.

Protección:

En cada proceso los registros son archivados en carpetas apropiadas para su conservación.
En medio electrónico se controlaran con claves de acceso de red y del software WINZIP.

Recuperación:

Para los formatos de registros electrónicos, se recuperaran con las respectivas claves de acceso, digitadas desde puntos autorizados de la red.

Los registros en copias duras, se recuperaran de la carpeta de archivo de acuerdo al proceso respectivo.

Tiempo de retención:

Para los registros el tiempo de retención se estima de acuerdo a lo estipulado en el listado maestro de control de registros.

Tipo de Disposición:

Los registros electrónicos estarán disponibles en la red.
Los registros de copia dura estarán disponibles en carpetas en las áreas respectivas.

Nota: Los registros deben ser legibles.

DOCUMENTOS RELACIONADOS:

Procedimiento de control de registros

REGISTROS:

Listado maestro de control de registros.

ANEXOS:

No Aplica.

14. PROCEDIMIENTO REVISION GERENCIAL

OBJETO: Establecer los lineamientos para llevar a cabo las revisiones al Sistema de Gestión de Seguridad de la Información en el área contable de la ESE hospital Local de Rio de Oro Cesar por parte de la Gerencia y Junta Directiva de la institución y asegurar asi la conveniencia, eficacia y seguridad del sistema

ALCANCE: Para todo el personal del área contable que integra el SGSI

DEFINICIONES:

Alta dirección: gerencia – junta directiva de la ESE personas que dirigen y controlan el más alto nivel de la organización

Revisión: actividad emprendida para asegurar la conveniencia adecuación y eficacia del tema objeto de la revisión para alcanzar los objetivos establecidos

RESPONSABLES:

Gerente general y Junta Directiva: responsable de hacer las revisiones gerenciales

CONTENIDO: la revisión gerencial del Sistema de Gestión de seguridad de la información deben cumplir con:

Programas juntas de revisión por la dirección, difundir y socializar

Revisar toda la información de entrada durante la junta de revisión por la dirección

Tomar decisiones y documentar los resultados

Elaborar y distribuir minuta de revisión por la dirección y planear ejecución de acciones

Realizar cambios a la estructura documental y controlar versiones

Dar seguimiento a acciones a realizar y evaluar el impacto de la seguridad de la información en el área contable de la ESE

DOCUMENTOS RELACIONADO

Procedimiento de revisión Gerencial

REGISTROS:

Informe de revisión gerencial

ANEXOS:

No Aplica.

5. CONCLUSIONES

Se realizó un modelado de negocio donde se definieron los procesos que se llevan a cabo en el Área de contabilidad de la E.S.E, identificando la cadena de valor, modelando sus procesos a través del BMM (Business Motivation Model), creando su estructura orgánica e identificando la Tecnología de Información (TI).

La auditoría administrativa y de sistemas de información realizada en el área de contabilidad de la E.S.E, logro identificar falencias y vulnerabilidades que fomentan el riesgo de la perdida, daño o mal funcionamiento de la información física y lógica del Área, estas vulnerabilidades fueron consolidadas en una matriz de riesgos, en la cual se identificaron los controles necesarios que permitirán la mitigación de los mismos.

Tomando como marcos de referencia, normas o buenas prácticas, se identificaron COBIT 4.1, NTC-ISO/IEC 27001 y NTC-ISO/IEC 27002, mostrando un comparativo entre las mismas y de acuerdo a la necesidad encontrada en el Área de Contabilidad que justifique establecer un Sistema de Gestión de Seguridad de la Información, se tomó como base la norma NTC-ISO/IEC 27001 que ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información y la NTC-ISO/IEC 27002 puesto que permite buenas prácticas para salvaguardar la información.

La política de seguridad establecida como base para el Sistema de Gestión de Seguridad de la Información diseñado para el Área de Contabilidad de la E.S.E, se realizó bajo los términos de las características del Área, su ubicación, activos y tecnología. Se encuentra estructurada con una resolución y tres capítulos, detallando en el primer capítulo los tres dominios referentes a la parte organizacional, en el capítulo dos siete dominios referentes a la protección de la información y el último capítulo está conformado por un glosario y un historial de revisiones, aprobaciones y actualizaciones.

La importancia de la implementación del sistema de gestión de seguridad de la información en el Área contable se ve reflejada al realizar el diseño según la norma ISO/IEC 27001:2005 aplicando todos sus controles en cada uno de sus procesos contables y realizando todos los seguimientos acordes a lo establecido en dicha norma.

RECOMENDACIONES

Implementación del sistema de gestión de seguridad de la información para el Área de contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar.

Los auditores no deben realizar auditorías a las actividades o procesos por los cuales son responsables directos, con el fin de no afectar la objetividad.

La auditoría interna se realizará con una frecuencia mínima anual (un ciclo).

Las Auditorias deben ser realizadas por auditores internos o externos, siempre y cuando cumplan con el nivel de competencias definido para los auditores internos de seguridad en la Información

REFERENCIAS BIBLIOGRÁFICAS

CORLETTI, ALEJANDRO. ISO/IEC 27001. Los Controles – 2006 [en línea]. http://www. kriptopolis.org/iso-27001-los-controles-parte-II

MARIO TAMAYO Y TAMAYO, 2003. El Proceso de la Investigación Científica 4 Edición. Limusa Noriega Editores.

IT GOVERNANCE INSTITUTE. COBIT 4.1.pdf - 2007 [en línea] http://www.isaca.org

INTERNATIONAL ORGANIZATIÓN FOR STANDARIZATION. ISO/IEC 27001:2005 [en línea]. http://www.iso.org/iso/home/search.htm?qt=iso+27001&published=on&active_tab=standards&sort_by=rel

INTERNATIONAL ORGANIZATIÓN FOR STANDARIZATION. ISO/IEC 27002:2005 Tecnología de la información - Técnicas de seguridad - Código de buenas prácticas para la gestión de seguridad de la información. [en línea]. http://www.iso.org/iso/home/search.htm?qt=iso+27002&sort=rel&type=simple&published=on

ADMINISTRACIÓN DE RIESGOS AS/NZS 4360. 2004 [en línea]. http://www.mwds.com/AS4me_files/AS-NZS%204360-2004%20Risk%20Management.pdf

IT GOVERNANCE INSTITUTE (ITGI) y OFICINA GUBERNAMENTAL DE COMERCIO (OGC). Alineando COBIT 4.1, ITIL v3 e ISO/IEC 27002 en Beneficio del Negocio. 2008. 130 h. [en línea]. http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2,7.pdf.

OSIATIS. [en línea]. http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_continuidad_del_servicio/proceso_gestion_de_la_continuidad_del_servicio/analisis_impacto_continuidad_del_servicio.php

ROMERO, Sara M y NAVARRO, Henry E. Módulo Evaluación de la Seguridad de la Información. Especialización en Auditoria de Sistemas, Universidad Francisco de Paula Santander Ocaña. 2012.

GESTIÓN DEL SGSI CON LA HERRAMIENTA – Soluciones de Seguridad [en línea]. http://www.siainternational.com/noticias/sgsi.pdf

NTC-ISO/IEC 27005, Tecnología de la información. Código de práctica para la gestión de la seguridad de la información.

ÁLVAREZ ZURITA, Flor M y GARCÍA GUZMÁN, Pamela A. Implementación de un Sistema de Gestión de Seguridad de la Información basada en la norma ISO 27001. Para la Intranet de la Corporación Metropolitana de Salud. Quito, Ecuador. 2007. 298 h. Escuela Politécnica Nacional. [en línea]. http://bibdigital.epn.edu.ec/handle/15000/565

VASCO AGUAS, Mireya I y VERDEZOTO SALTOS, Mercedes E. Plan de Gestión de Seguridad de la Información basado en TIC'S para la Facultad de Ingeniería de Sistemas de la Escuela Politécnica Nacional. Quito, Ecuador.. 2009. 226 h. Escuela Politécnica Nacional. [en línea]. http://bibdigital.epn.edu.ec/handle/15000/4370?mode=full

ORTEGA PACHECO, Oscar R. Centro de investigaciones económicas, administrativas y sociales, Gestión de la Seguridad de la Información en la Empresa. México D.F. 2010. 90h. Instituto Politécnico Nacional. [en línea]. http://www.repositoriodigital.ipn.mx/handle/123456789/6564

CAMPAÑA TENESACA, Oscar E. Plan de Propuesta para la Implantación de la Norma de Seguridad Informática ISO 27001:2005, para el Grupo Social Fondo Ecuatoriano Populorum Progressio (GSFEPP). Quito, Ecuador. 2010. 207h. [en línea] http://dspace.ups.edu.ec/handle/123456789/4468?mode=full

VILLENA AGUILAR, Moises A. Sistema de Gestión de Seguridad de la Información para una Institución Financiera. Lima, Perú. 2006. 72h. Pontificia Universidad Católica del Perú. [en línea] http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/362/VILLENA_MOIS%C3%89S_SISTEMA_DE%20GESTI%C3%93N_DE_SEGURIDAD_DE_INFORMACI%C3%93N_PARA_UNA_INSTITUCI%C3%93N_FINANCIERA.pdf

BELTRAN, Gustavo. Consultoría Estratégica y coachig de negocios. [En línea] [Citado el: 28 de 01 de 2013.] http://gustavobeltran.com/%C2%BFque-se-entiende-por-direccionamiento-estrategico/.

JIMENEZ RUIZ, Alberto. myEchelon: Un sistema de Auditoría de Seguridad Informática Avanzado bajo

GNU/Linux. Universidad de Almería. Almería, España. 217 h. [en línea]. http://www.adminso.es/images/9/9c/Alberto_PFC.pdf.

Plantilla para aplicar el ciclo PHVA. Tomado de: http://www.negociosyemprendimiento.org/2010/08/plantillapara-aplicar-el-ciclo-phva-de.html

REFERENCIAS DOCUMENTALES ELECTRONICAS

NOXGLOBE. Conozca COBIT [en línea]. http://www. noxglobe.com/modules/articles/cobit/

INTERNATIONAL ORGANIZATIÓN FOR STANDARIZATION. ISO/IEC 27000 – 2008 [en línea]. http://www.iso27000.es

ORGANISMO INTERNACIONAL DE CERTIFICACIÓN DE AUDITORES DE SISTEMAS DE GESTIÓN (IRCA). ISO 27002 vs. COBIT - Planificación de la Seguridad de la información. 2013. [en línea]. https://www.google.com.co/search?q=ISO+27002+vs.+COBIT++Planificaci%C3%B3n+de+la+seguridad+de+la+informaic%C3%B3n&oq=ISO+27002+vs.+COBIT++Planificaci%C3%B3n+de+la+seguridad+de+la+informaic%C3%B3n&aqs=chrome.0.57j60l2.2033j0&sourceid=chrome&ie=UTF-8.

SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN PARA LA GESTIÓN. [en línea]. http://riunet.upv.es/handle/10251/8374

SGSI – Sistema de Gestión de Seguridad de la Información [en línea]. http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/

SEGURIDAD DE LA INFORMACIÓN EN COLOMBIA. [en línea]. http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – Universidad Tecnológica de Pereira [en línea]. http://sgsi.utp.edu.co/

ANEXOS

Anexo A. Auditoria administrativa y sistemas de información del Área de contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar.

ENCUESTA		
Objetivo: recopilar información para evaluar administrativamente y los sistemas de información del área contable de la ESE Hospital Local de Rio de Oro cesar		
Nombre del encuestado	**Cargo del encuestado**	**Teléfono del encuetado**
Carlos Fernando Lemus	Jefe Administrativo Y Financiero	3128761238

Auditoria Administrativa al área Contable de la ESE Hospital Local de Rio de Oro cesar	Calificar el grado de cumplimiento	
Preguntas	**SI**	**NO**
Conoce la misión, visión. Valores y principios de la ESE	**X**	
Cuenta con un objetivo definido para la realización de su trabajo en el área contable de la ESE?	**X**	
¿Sabe usted si la empresa cuenta con unidades de medida para cuantificar el avance de sus acciones?		**X**
¿Cuenta con un programa de trabajo?		**X**
¿Están claramente delimitadas sus funciones?	**X**	
¿Existe duplicidad de funciones?		
¿El ambiente laboral de la empresa es bueno?	**X**	
¿El ambiente laboral de la empresa es Malo?		**X**
Tiene indicadores para medir el proceso del área contable		
Se realizan avaluaciones contables		**X**
Los actividades del área contable se encuentran bien definidos		**X**

LISTA DE CHEQUEO – auditoria Administrativa – área de contabilidad
Nombre de la Empresa: ESE Hospital Local de Rio de Oro Cesar
Fecha: 14 de Julio de 2013 a 14 de agosto de 2013

Evaluar el funcionamiento administrativo del área contable de la ESE Hospital Local de Rio de Oro Cesar	
Descripción de Concepto	**Cumple**
La ESE Hospital Local de Rio de Oro tiene definido la misión, visión, principios y calores del área contable?	**SI**
La misión, visión. Principios y valores del área contable de la ese se pueden medir?	**SI**
Los objetivos del área contable se han definido con los objetivos generales de la ESE	**SI**
Se han definido Factores Claves de éxitos para lograr los objetivos propuestos en la ESE	**SI**
Se definieron indicadores para verificar el cumplimiento de los objetivos	**NO**
La ESE tiene definida políticas sobre el riesgo y controles en los niveles de operaciones del área contable y están modificadas de acuerdo a las necesidades	**NO**
Se vigila el ambiente interno del área contable dentro de la ESE	**NO**
Los impactos financiero son calificados periódicamente	**NO**
Está definido el nivel de autoridad	**NO**
Se han implementado canales de comunicación efectivos	
Se mide el rendimiento de la organización	**NO**
Existe un plan de recurso humano alineado con los objetivos y las estrategias de la ESE	**NO**
El área cuenta con procedimientos que le permitan identificar las necesidades de capacitación de sus empleados teniendo en cuenta los objetivos	**NO**
El desempeño de los empleados es medido por lo menos una vez al año	**NO**
Se monitorea el clima organizacional	**NO**
Existen planes de crecimiento dentro de la ESE para los empleados	**NO**
Se promueve la satisfacción de los empleados	**NO**
Están identificados los riesgos que impidan el logro de los objetivos en el área contable	**NO**
Se mide el rendimiento del proceso contable, costos, calidad, tiempos.	**NO**
Las actividades de control en el área contable se vigilan de forma permanente	**NO**
Los procesos en el área contable están documentados y se revisan de forma permanente para actualizarlos y mejorarlos	**NO**
Existen canales de comunicación donde los que interviene en el proceso contable den sus sugerencias para el mejoramiento del proceso	**NO**
Las reciben las quejas y se les hace tratamiento referentes al proceso contable	**NO**
Se han desarrollado programas de mejoramiento continuo de la Calidad	**NO**

LISTA DE CHEQUEO auditoria Sistemas de Información – área de contabilidad
Nombre de la Empresa: ESE Hospital Local de Rio de Oro Cesar
Fecha: 14 de Julio de 2013 a 14 de agosto de 2013

Evaluar el funcionamiento de los sistemas de información del área contable de la ESE Hospital Local de Rio de Oro Cesar	
Descripción de Concepto	**Cumple**
Seguridad en la protección y conservación de locales, instalaciones, mobiliario y equipos	
Las condiciones generales de trabajo de los sistema computacionales del área contable son cómodas para el usuario del sistema	**SI**
Tiene protección contra la humedad en el ambiente	**NO**
Toman medidas para prevenir que los sistemas computacionales y las instalaciones eléctricas, telefónicas del área contable tengan contacto con el agua	**NO**
Tienen protección contra partículas de polvo desechos volátiles de cualquier tipo a fin de evitar desperfectos en los sistemas computacionales en el are contable de la ESE	**NO**
Tiene análisis de los sistemas de acomodación y pisos falsos	**NO**
Análisis de regulación de temperatura y aire acondicionado	**NO**
Análisis de regulación de la humead en el medio ambiente del área contable	**NO**
Análisis de suministros de energía, comunicación y procesamiento de los datos	**NO**
Análisis de limpieza del área contable	**NO**
La iluminación artificial del área Contable y la iluminación por medio de luz solar.	**NO**
Las instalaciones eléctricas, de datos y de comunicación	**NO**
Los accesos y salidas en las áreas contable	**SI**
La repercusión de los aspectos de carácter ergonómico.	**NO**
Las adaptaciones de los equipos de cómputo.	**SI**
Las condiciones de trabajo con computadora.	**SI**
Protección contra contingencias causadas por la temperatura del sistema de aire acondicionado.	**SI**
La ventilación natural de las áreas y espacios	**SI**
Seguridad en la información del Área contable y bases de datos	
El rendimiento y uso del sistema computacional y de sus periféricos asociados es adecuado	**NO**
La existencia, protección y periodicidad de los respaldos de bases de datos, software e información importante del área contable está bien definida.	**NO**
La configuración, instalaciones y seguridad del equipo de cómputo, mobiliario y demás equipos del área de contable se encuentran de una	**NO**

forma adecuada y protegen la información	
El rendimiento, la aplicación y la utilidad del equipo de cómputo, mobiliario y demás equipos del área contable son los adecuados	**NO**
Evaluar la seguridad en el procesamiento de información.	**NO**
Evaluar los procedimientos de captura, procesamiento de datos y emisión de resultados de los sistemas computacionales	**NO**
Evaluar el estado físico de los sistemas	**NO**

Auditores:

Aura Lucia Casadiegos Santana – Ingeniera Industrial
Marcela Quintero – Comunicadora Social
Mileidy Toro Rueda – Ingeniera de Sistemas

SITUACIONES ENCONTRADAS

Situaciones	Causas	Soluciones
no implementación de sistemas de tecnología de la información de la ESE	No organización de los procesos de la ESE	Implementar sistemas que garanticen el manejo adecuado de los procesos
Equipos obsoletos y con software desactualizados	Falta de presupuesto para compra de equipos y actualización del software	Buscar presupuesto y realizar proyectos para la compra de equipos y actualización del software contable
No existen mantenimiento de equipos ni preventivos ni correctivos	Falta de organización del proceso de infraestructura y equipos médicos	Implementar programa de mantenimiento preventivo y correctivo en la ESE
Falta de capacitación del personal que labora en la ESE	falta de organización del proceso de recursos humanos	Implementar capacitaciones al personal del área contable de la ESE
Los procesos no se encuentran definidos y organizaciones ni las actividades del área contable	Falta de planeación estratégica de la ESE	Implementar un sistema que garantice la ejecución de los procesos y la confiabilidad en la tecnología d la información del área contable de la ESE
Falta de comunicación entre el área contable – presupuesto – almacén	Falta de capacitación	Realizar programa de capacitación al área contable de la ESE

Elaboro: firma y fecha
Mileidy Toro Rueda
Marcela Quintero
Aura lucia Casadiegos

SITUACIONES ENCONTRADAS EN LA AUDITORIA PARTE ADMINISTRATIVA Y DE SISTEMAS DE INFORMACIÓN DEL ÁREA CONTABLE DE LA ESE HOSPITAL LOCAL DE RIO DE ORO CESAR

Empresa: E.S.E Hospital Local de Rio de Oro Cesar	**Área Auditada:** Área de contabilidad	**Fecha de auditoría:** 14 de Julio de 2013 al 14 Agosto de 2013 **Fecha de entrega de informe Final:** 15 de Julio de 2013		
Situaciones	**Causas**	**Soluciones**	**Fecha de Solución**	**Responsable**
En los sistemas de información encontramos que no se encuentra implementado un sistema de información que garantice la mitigación de los riesgos que pueden general la no protección de la información	Las principal causa de que en el área contable de la ESE estén ocurriendo las situaciones encontradas en la auditoria es el desconocimiento total de los sistemas te tecnología de la información y nivel de implementación 0	Implementar unas sistema que garantice la tecnología de información del área contable en la ESE	Diciembre de 2014	Gerencia y director administrativo y financiero
La no actualización del software contable no garantiza que los sistemas de información y administrativos sean confiables Desconocimiento del modelo de TI como pieza fundamental en el correcto funcionamiento de la información que genera la ESE	La falta de equipos y la desactualización del software contable TNS	Actualización de software y compra de equipos.	Diciembre de 2013	Gerente y jede del área de contabilidad.

En el área administrativa no tiene un sistema de información estructurado por lo cual los procesos no son eficaces n				

Elaboro: firma y fecha
Mileidy Toro
Marcela Quintero
Aura lucia Casadiegos

INFORME FINAL

AUDITORIA DE SISTEMAS
Auditores A & M2

Ocaña, 29 de julio de 2013

Doctor:
ISSAC RAFAEL CERVANTEZ BARRIOS
Gerente ESE Hospital Local de Rio de Oro Cesar

Atentamente me permito remitir el informe del resultado de la auditoría realizada al área Contable de la ESE la cual usted representa la cual se realizó del **1 de julio al 30 de julio** del año en curso.

Gracias por su atención y colaboración

Atentamente.

AURA LUCIA CASADIEGOS
MARCELA QUINTERO
MILEYDY TORO RUEDA

DICTAMEN DE AUDITORIA DE SISTEMAS AREA CONTABLE ESE HOSPITAL LOCAL DE RIO DE ORO CESAR

Ocaña, 29 de julio de 2013

Doctor:
ISSAC RAFAEL CERVANTEZ BARRIOS

Gerente ESE Hospital Local de Rio de Oro Cesar

Debido a que el proceso más crítico y complejo de la ESE es el contable ya que sus actividades debe estar muy bien documentados y protegidas se decidió hacer una auditoria de sistemas de la información y administrativa a esta área ordenada por el auditor de la institución la cual tuvo fecha de inicio el 26 de junio de 2013 y finalización el 10 de julio del mismo año

En la auditoria se evaluó el proceso administrativo y de sistemas de información del área contable de la ESE Hospital Local de Rio de Oro observando la falta de sistemas de tecnología de la información y falta de implementación de los procesos administrativos

Como auditores recomendación documentar los procesos administrativos del Sistema contable de la ESE y comenzar con la implementación de un sistema de garantía de tecnología de la información como lo mostramos en las tablas anexas a este informe

Gracias por su atención y colaboración

Atentamente.

AURA LUCIA CASADIEGOS
MARCELA QUINTERO
MILEIDY TORO RUEDA