TECNICAS DE AUDITORIA DE SISTEMAS APLICADAS AL PROCESO DE CONTRATACION Y PAGINAS WEB EN ENTIDADES OFICIALES DEL DEPARTAMENTO DE NARIÑO

LUIS CARLOS CHAVES YELA
RICARDO ALEXANDER CABRERA SOLARTE

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2010

TECNICAS DE AUDITORIA DE SISTEMAS APLICADAS AL PROCESO DE CONTRATACION Y PAGINAS WEB EN ENTIDADES OFICIALES DEL DEPARTAMENTO DE NARIÑO

LUIS CARLOS CHAVES YELA
RICARDO ALEXANDER CABRERA SOLARTE

TRABAJO DE GRADO PRESENTADO COMO REQUISITO PARCIAL PARA OPTAR AL TITULO DE INGENIERO DE SISTEMAS

Director
ING. MANUEL BOLAÑOS GONZALES

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2010

NOTA DE RESPONSABILIDAD

Las ideas y conclusiones aportadas en este Trabajo de Grado son responsabilidad de los autores.

Artículo 1 del Acuerdo No. 324 de octubre 11 de 1966, emanado del honorable Consejo Directivo de la Universidad de Nariño.

NOTA DE ACEPTACIÓN

_____

_____

_____

_____
Jurado

_____
Jurado

San Juan de Pasto, 2010

AGRADECIMIENTOS

A Dios por ser la luz en el camino que emprendimos cuando comenzamos nuestra carrera.

Al ingeniero Manuel Bolaños por su compromiso y entrega que fueron fundamentales en el proceso que hoy culminamos.

A nuestras familias parte fundamental de nuestras vidas a quienes les debemos todos nuestros logros.

A nuestros amigos por el apoyo recibido.

DEDICATORIA

A los amigos, familiares y profesores por ser parte de nuestra formación como Ingenieros.

RESUMEN

El proceso de auditoria es fundamental en cualquier entidad para mejorar sus procesos y tener mayor control de su funcionamiento. Por esta razón, existen entidades gubernamentales encargadas de auditar las empresas que manejan recursos o procesos del estado; una de esas entidades es la Contraloría Departamental de Nariño.

Este trabajo es la ejecución de una auditoria realizada al Hospital Universitario Departamental de Nariño E.S.E y el Hospital Civil de Ipiales E.S.E, esta auditoria se realizó con el fin de identificar las vulnerabilidades del proceso de contratación tanto física como lógicamente, además se evaluó el cumplimiento del decreto 1151 de 2008 concerniente a Gobierno en Línea, requisito de la Contraloría para las entidades del Departamento.

Este proceso se realizo dentro del marco de referencia “COBIT”, del cual se seleccionaron diferentes procesos y objetivos de control.

Después del proceso de auditoria se prosiguió con la evaluación de la pagina web de las entidades; culminando este proceso con la formulación de recomendaciones para el mejoramiento del proceso de contratación y del cumplimiento del decreto 1151 de 2008 de Gobierno en Línea.

ABSTRACT

The audit process is fundamental in any organization to improve its processes and to have major control of its operation. For this reason, exist governmental organizations in charge to audit the companies that handle state's resources or processes; one of those organizations is the Contraloria Departamental de Nariño.

This assignment is the execution of an audit realized to the Hospital Universitario Departamental de Nariño E.S.E and to the Hospital Civil de Ipiales E.S.E. This audit was realized with the purpose of identify the vulnerabilities of the hiring process in aspects such as physical and logical. Furthermore, was evaluated the fulfilment of decree 1151 of 2008 concerning Government in line, requirement of the Contraloría for the organizations of the Department.

This process was executed within the frame of reference "COBIT", of which to different processes and objectives from control were selected.

After the audit process, was continued with the evaluation of the organization's Web side. Culminating this process, with the formulation of recommendations for it improvement in the hiring process and the fulfilment of decree 1151 of 2008 of Government in line.

TABLA DE CONTENIDO

GLOSARIO 13

INTRODUCCION 20

1. MARCO TEORICO 25
1.1. ANTECEDENTES 25
1.2. ASPECTOS GENERALES SOBR AUDITORIA: 27
1.3. EL AUDITOR 31
1.4. TIPOS DE AUDITORIA: 32
1.4.1 .Auditoria Fiscal: 33
1.4.2. Auditoria Financiera 33
1.4.3 Auditoria Operacional: 33
1.4.4. Auditoria Administrativa: 34
1.4.5. Auditoria Integral 36
1.4.6 .Auditoria de Sistemas 37
1.5. AUDITORIA DE SISTEMAS COMO OBJETO DE ESTUDIO 39
1.5.1 .Alcance de la auditoria de sistemas 39
1.5.2 . Objetivos de la auditoria de sistemas 40
1.5.3 Principales pruebas y herramientas para efectuar una auditoria de sistemas 40
1.5.4 Perfiles profesionales de los auditores informaticos 40
1.5.5 Pasos a seguir para una auditoria de sistemas en una organizacion 42
1.6 . METODOLOGIAS DE AUDITORIA DE SISTEMAS 47
1.6.1. COBIT (Control Objectives for Information and Related Technology) 48
1.6.2 .COSO (Sponsoring Organizations of the Treadway Commission) 78
1.7 ..TÉCNICAS DE AUDITORIA DE SISTEMAS 79
1.7.1 .. Selección de areas de auditoria 79
1.7.2 Técnicas para operacionalizar la función de auditoria 80
1.7.3 Técnicas para probar controles de sistemas en funcionamiento 81
1.7.4 Técnicas para seleccionar y monitorear transacciones 86
1.7.5 Técnicas para la auditoria de la información almacenada 90
1.7.6 Técnicas para examinar programas aplicativos 96

2 METODOLOGIA 101

3. . DESARROLLO DEL TRABAJO 104
3.1 ARCHIVO PERMANENTE 104
3.1.1. Leyes y decretos comunes 104
3.1.2. Hospital Universitario Departamental de Nariño E.S.E 104

3.1.3. Hospital Civil de Ipiales E.S.E 135
3.2. .ARCHIVO CORRIENTE 154
3.2.1. Programa de auditoria 154
3.2.2.. Diseño de los elementos de auditoria: 165
3.2.3 Hallazgos 176
3.2.4 Informe de auditoria 232
4. CONCLUSIONES 280
RECOMENDACIONES 281
BIBLIOGRAFIA 282
ANEXOS .....

LISTA DE TABLAS.

Tabla 1 Perfiles Profesionales y Actividades..... 40
Tabla 2 Cuadro de definición de fuentes de conocimiento, pruebas de auditoria .... análisis de auditoria..... 167
Tabla 3 Cuestionario Cuantitativo 170
Tabla 4 Matriz de probabilidad de ocurrencia e impacto según relevancia del ..... proceso..... 172
Tabla 5 Hallazgo 1 HD 176
Tabla 6 Hallazgo 2 HD 178
Tabla7 Hallazgo 3 HD 181
Tabla8 Hallazgo 4 HD 183
Tabla9 Hallazgo 5 HD 185
Tabla10 Hallazgo 6 HD 187
Tabla11 Hallazgo 7 HD 190
Tabla12 Hallazgo 8 HD 192
Tabla13 Hallazgo 9 HD 194
Tabla14 Hallazgo 10 HD 196
Tabla15 Hallazgo 11 HD 197
Tabla16 Hallazgo 12 HD 199
Tabla17 Hallazgo 13 HD 201
Tabla18 Hallazgo 14 HD 203
Tabla19 Hallazgo 1 HC 205
Tabla20 Hallazgo 2 HC 206
Tabla21 Hallazgo 3 HC 208
Tabla22 Hallazgo 4 HC 209
Tabla23 Hallazgo 5 HC 211
Tabla24 Hallazgo 6 HC 212
Tabla25 Hallazgo 7 HC 215
Tabla26 Hallazgo 8 HC 217
Tabla27 Hallazgo 9 HC 219
Tabla28 Hallazgo 10 HC 221
Tabla29 Hallazgo 11 HC 223
Tabla30 Hallazgo 12 HC 225
Tabla31 Hallazgo 13 HC 228
Tabla32 Hallazgo 14 HC 229
Tabla33 GL - HD 252
Tabla34 GL2 - HD 253
Tabla35 Usabilidad – HD 256
Tabla36 GL - HC 266
Tabla37 GL2 – HC 266

Tabla38 Usabilidad – HC 270

LISTA DE FIGURAS

Figura1 Las tres dimensiones conceptuales de COBIT 76
Figura2 Organigrama Hospital Civil de Ipiales E.S.E. 135
Figura3 Ref - Hallazgo 173
Figura4 Informacion General Hallazgo 173
Figura5 Descripción Hallazgo 173
Figura6 Consecuencias y Riesgos 174
Figura7 Recomendaciones 174
Figura8 Mapa del sitio HD 261
Figura9 Mapa del sitio2 HD 261
Figura10 Indice global HD 262
Figura11 Indice global2 HD 262
Figura12 Tabla c HD 263
Figura13 Navegabilidad HD 263
Figura14 Uniformidad HD 264
Figura15 Enlaces interes HD 264
Figura16 Profesionales HD 265
Figura17 Enlaces rotos HD 265
Figura18 HC – Usabilidad 276
Figura19 HC – Usabilidad2 277
Figura20 HC – Usabilidad3 277
Figura21 HC – Usabilidad4 277
Figura22 HC – Usabilidad5 278

GLOSARIO

ACTIVO: En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Según [ISO/IEC 13335-1:2004]: Cualquier cosa que tiene valor para la organización.

ALERTA: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

AMBIENTE: Es el medio en que se desarrollo una programación específica.

AMENAZA: Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

ANÁLISIS DE RIESGOS: Según [ISO/IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

APLICACIÓN: Tipo de programa específicamente dedicado al proceso de una función concreta dentro de la entidad.

AUDITOR: Persona capacitada y experimentada que se designa por una autoridad competente, para revisar, examinar y evaluar los resultados de la gestión administrativa y financiera de una dependencia o entidad.

AUDITORÍA: La auditoría puede definirse como un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados, cuyo fin consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen.

AUTENTICACIÓN: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

BASES DE DATOS: Colección de datos organizada de tal modo que el ordenador pueda acceder rápidamente a ella. Una base de datos relacionar es aquella en la que las conexiones entre los distintos elementos que forman la base de datos están almacenadas explícitamente con el fin de ayudar a la manipulación y el acceso a éstos.

CHECKLIST: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo.

COBIT: Objetivos de Control para la información y Tecnologías relacionadas (COBIT, en inglés: Control Objectives for Information and Related Technology) es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información, (ISACA, en inglés: Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: IT Governance Institute) en 1992.

CONFIDENCIALIDAD: Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

CONTRALORÍA DEPARTAMENTAL DE NARIÑO: Entidad que vigila la gestión fiscal de la administración pública y de los particulares o entidades que manejan fondos o bienes de la nación.

CONTROL: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida.

CONTROL CORRECTIVO: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

CONTROL PREVENTIVO: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

CRIPTOGRAFÍA: Ciencia dedicada al estudio de técnicas capaces de conferir seguridad a los datos.

DATOS: Información antes de ser procesada.

DESASTRE: Cualquier evento que interrumpe las operaciones o servicios habituales de una entidad durante el tiempo suficiente como para verse afectada de manera significativa.

DISPONIBILIDAD: Según [ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

EVALUACIÓN DE RIESGOS: Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

EVENTO: Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.

FACTIBILIDAD: Es la disponibilidad de los recursos necesarios para llevar a cabo los objetivos o metas señaladas, sirve para recopilar datos relevantes sobre el desarrollo de un proyecto y en base a ello tomar la mejor decisión.

GESTIÓN DE RIESGOS: Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

HARDWARE: Es la parte física de un computador y más ampliamente de cualquier dispositivo electrónico, usualmente este término es utilizado en una forma más amplia, generalmente para describir componentes físicos de una tecnología, así el hardware puede ser de un equipo electrónico, un equipo informático o un robot. En informática también se aplica a los periféricos de una computadora tales como el disco duro, CD-ROM, entre otros.

IMPACTO: El costo en términos cualitativos y cuantitativos que causo un problema en la entidad.

INCIDENTE: Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

INTEGRIDAD: Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

INTERNET: Interconexión de redes informáticas que permite a las computadoras conectadas comunicarse directamente.

INTRANET: Conjunto de contenidos compartidos por un grupo bien definido dentro de una organización, por ello sería lo opuesto al término Web (World Wide Web) formado por contenidos libremente accesibles por cualquier público. Tiene como función principal proveer lógica de negocios para aplicaciones de captura,

informes y consultas con el fin de facilitar la producción de dichos grupos de trabajo; es también un importante medio de difusión de información interna a nivel de grupo de trabajo

ISACA: Information Systems Audit and Control Association. Publica COBIT y emite diversas acreditaciones en el ámbito de la seguridad de la información.

METODOLOGÍA: Conjunto de métodos utilizados en la investigación científica

NORMA: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

OBJETIVO: Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad de TI determinada.

PASSWORD: Contraseña para equipo de cómputo o aplicación.

POLÍTICA DE SEGURIDAD: Según [ISO/IEC 27002:2005]: intención y dirección general expresada formalmente por la Dirección.

PROCEDIMIENTO: Modo de ejecutar determinadas acciones que suelen realizarse de la misma forma, con una serie común de pasos claramente definidos, que permiten realizar una ocupación, trabajo, investigación, o estudio correctamente.

PROCESAMIENTO DE DATOS: Conjunto de diferentes operaciones en secuencia sistemática sobre el dato, las cuales se basan en la elaboración, manipuleo y tratamiento del mismo, mediante máquinas automáticas para producir los resultados esperados.

PROCESO: Conjunto de operaciones lógicas y aritméticas ordenadas, cuyo fin es la obtención de resultados.

PROGRAMA: Secuencia de instrucciones que obliga al ordenador a realizar una tarea determinada.

RED: Servicio de comunicación de datos entre ordenadores.

REPOSITORIO: Donde se almacenan los elementos definidos o creados por la herramienta, y cuya gestión se realiza mediante el apoyo de un Sistema de Gestión de Base de Datos (SGBD) o de un sistema de gestión de ficheros

RIESGO: Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

SECOP: Sistema electrónico para la contratación publica.

SEGREGACIÓN DE TAREAS: Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

SELECCIÓN DE CONTROLES: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SERVICIOS DE TRATAMIENTO DE INFORMACIÓN: Según [ISO/IEC 27002:2005]: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento.

SERVIDOR: Conjunto de hardware acompañado de sistema operativo especial para ser utilizado por múltiples usuarios, que ofrece una variedad de servicios a usuarios locales o foráneos que utilizan una o muchas aplicaciones.

SICE: Sistema de información que integra todos los datos relevantes de proceso de contratación estatal, permitiendo su autorregulación, control institucional y publicidad de las operaciones.

SISTEMA DE INFORMACIÓN: Se denomina Sistema de Información al conjunto de procedimientos manuales y/o automatizados que están orientados a proporcionar información para la toma de decisiones.

SOFTWARE: Componentes inmateriales del ordenador: programas, sistemas operativos, etc.

TI: Tecnologías de Información

TÉCNICA: La técnica es el procedimiento o el conjunto de procedimientos que tienen como objetivo obtener un resultado determinado, ya sea en el campo de la ciencia, de la tecnología, de las artesanías o en otra actividad

TRATAMIENTO DE RIESGOS: Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

VALORACIÓN DE RIESGOS: Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

VULNERABILIDAD: Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

INTRODUCCION

Actualmente los sistemas de información y las tecnologías de información han cambiado la forma en que operan las organizaciones. A través de su uso se logran importantes mejoras, pues automatizan los procesos operativos, suministran una plataforma de información necesaria para la toma de decisiones y lo más importante su implantación logra ventajas operativas que se traducen en beneficios para las instituciones o empresas.

La seguridad de la información debe ser un proceso integrado. Esto quiere decir que con el uso de controles técnicos, administrativos y físicos, se debe lograr la confianza en los sistemas y garantizar que cumplan con los parámetros de: disponibilidad, integridad, confidencialidad, confiabilidad y desempeño.

Por otra parte, el gobierno propone ciertos lineamientos a los cuales las entidades públicas deben acogerse, como es el caso de los portales Web, con dichos portales se busca utilizar los recursos de sistemas ya existentes con el objetivo de prestar un mejor servicio a la comunidad.

Desde el punto de vista de los sistemas de información se presenta un proyecto para identificar por medio de un trabajo de auditoría de sistemas los diferentes hallazgos y vulnerabilidades de seguridad física y lógica, a las cuales se encuentra expuesta la información que manejan diariamente las entidades públicas del Departamento de Nariño, para desempeñar a cabalidad sus funciones y brindar un adecuado servicio a la comunidad.

El presente documento se organiza de la siguiente forma: en la primera parte se plantea el problema y su sistematización, se plantean los objetivos que se pretenden alcanzar luego se hablan de los antecedentes directamente relacionados con el proyecto, de la factibilidad y la metodología a seguir. En la última parte se especifican los recursos que se van a utilizar así como la distribución en tiempo de las tareas que están programadas para realizarse.

- **IDENTIFICACION DEL PROBLEMA**

o **TITULO DEL PROYECTO.** TECNICAS DE AUDITORIA DE SISTEMAS APLICADAS AL PROCESO DE CONTRATACIÓN Y PAGINAS WEB EN ENTIDADES OFICIALES DEL DEPARTAMENTO DE NARIÑO

o **LINEA DE INVESTIGACION.** Este proyecto corresponde a la línea de investigación Sistemas Computacionales.

- **DESCRIPCION DEL PROBLEMA**

o **Planteamiento del Problema.** La Contraloría Departamental de Nariño, es la encargada de realizar un seguimiento a las entidades públicas del Departamento, con el fin de garantizar el buen uso de los recursos asignados por el Gobierno, de igual forma es de vital importancia que la seguridad de la información que cada entidad pública maneja sea confiable e integra.

Hasta la fecha las entidades públicas no han sido sometidas a ningún tipo de proceso o estudio para identificar los posibles hallazgos y vulnerabilidades lógicas y físicas más relevantes que violen los lineamientos establecidos en el Decreto 1151 del 2008, que hace referencia al manual de implementación de la estrategia de gobierno en línea. Otro elemento importante es verificar como se lleva a cabo la contratación por cada una de las entidades públicas.

Actualmente la Contraloría Departamental Nariño no cuenta con un documento que permita corroborar el manejo correcto de los recursos por parte de las entidades públicas.

o **Formulación del Problema.** ¿Cómo realizar la evaluación de los procesos que garantizan el buen uso de los recursos, la implementación del portal Web y la información que se maneja en las entidades públicas, para establecer los riesgos más relevantes a los que se encuentran expuestas y recomendar los ajustes pertinentes?

o **Sistematización del Problema.**

- ¿Cómo realizar la evaluación del sitio Web de las entidades públicas del Departamento de Nariño, para identificar el cumplimiento del Decreto 1151 del 2008 sobre Gobierno en Línea?

- ¿Cómo se encuentran las condiciones de seguridad lógica de la información del proceso de contratación (TI) en las entidades públicas del Departamento de Nariño?

- ¿Cómo están las condiciones de seguridad física de la información del proceso de contratación (TI) en las entidades públicas del Departamento de Nariño?

- ¿Cómo realizar la evaluación de los controles que garantizan la seguridad física y lógica de la información que maneja el proceso de contratación (TI) en las entidades públicas del Departamento de Nariño para establecer los riesgos a los que se encuentra expuesta y recomendar controles para su protección?

- **OBJETIVOS**

o **Objetivo General.** Aplicar técnicas de auditoría de sistemas a entidades públicas del Departamento de Nariño para evidenciar vulnerabilidades de seguridad física y lógica a las que se encuentra expuesta la información manejada en el proceso de contratación (TI), y el cumplimiento del Decreto 1151 de 2008 sobre Gobierno en Línea.

- **Objetivos Específicos**

  - Analizar diferentes técnicas de auditoria de sistemas para determinar cuales deben ser utilizadas en cada una de las entidades tomadas como caso de estudio.

  - Auditar el sitio Web de las entidades públicas del Departamento de Nariño tomadas como caso de estudio.

  - Auditar el proceso de contratación (TI) de las entidades públicas del Departamento de Nariño tomadas como caso de estudio.

  - Aportar información que permita a las entidades auditadas implementar las medidas necesarias, para garantizar que los tramites realizados por

sus usuarios tengan como materia prima información confiable, integra y confidencial, que asegure la trasparencia en los procesos.

- **JUSTIFICACION**

"*La auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de computo, su utilización, eficiencia y seguridad, de los elementos de una organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alterativos se logre una utilización más eficiente de la información que servirá para una eventual toma de decisiones*."[1]

La auditoria de sistemas es de gran importancia para el excelente desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un excelente nivel de seguridad.

Para ayudar a cumplir a cabalidad las funciones de la Contraloría Departamental Nariño, en el control que ejercen sobre las entidades públicas del Departamento de Nariño, es justificable la aplicación de medidas y estrategias para asegurar el adecuado y transparente manejo de los recursos asignados y la información que está a cargo de dichas entidades.

Por lo anterior, el proceso de auditoría de sistemas se convierte en elemento fundamental y de vital importancia, para determinar los hallazgos y vulnerabilidades más relevantes de seguridad física y lógica que actualmente se presentan en el sistema de contratación, además, poder determinar si el sitio web de las entidades cumplen con los lineamientos del Decreto 1151 de 2008 de la estrategia de Gobierno en Línea.

Con la ejecución de la auditoria se beneficiarán los diferentes usuarios de estas entidades, ya que con base en los resultados presentados se podrán tomar las medidas necesarias, que permitan optimizar cada una de las tareas relacionadas con el procesamiento de la información.

[1] ECHENIQE GARCIA José A., Auditoría en informática, segunda edición [2a] Ed., Mc Graw Hill D. F. 2005.

- **ALCANCE Y DELIMITACION**

En el desarrollo de este proyecto se identificaron diferentes técnicas de auditoría de sistemas, y se utilizo la más adecuada en cada uno de los casos de estudio.

La aplicación de técnicas de auditoría de sistemas se realizo al proceso de contratación (TI) del Hospital Universitario Departamental de Nariño E.SE y del Hospital Civil de Ipiales E.S.E, con esto se identifico, comprobó y evaluó las vulnerabilidades de seguridad física y lógica a las que se encuentra expuesta la información que utilizan dichas entidades. Además, se audito el sitio Web de las entidades y se verifico si cumplían con los lineamientos del Decreto 1151 de 2008 de la estrategia de Gobierno en Línea.

Las entidades a auditar fueron:

- Hospital Universitario Departamental de Nariño E.S.E
- Hospital Civil de Ipiales E.S.E

Finalmente los resultados de este proceso se plasmaron en este informe que servirá para que estas entidades, tomen medidas preventivas y correctivas que subsanen los problemas detectados.

1. MARCO TEORICO

1.1. ANTECEDENTES

La auditoria de los sistemas de información ha surgido cuando las empresas e instituciones han tomado conciencia de que los datos que adquieren, conservan, procesan y emiten, es vital para su propia supervivencia diaria y proyección de eficiencia.

Por tanto, han elevado a la categoría de sistemas críticos prácticamente todos los sistemas internos que manejan información en uno solo, denominado sistema de información. En consecuencia por su naturaleza crítica el enfoque de auditoría debe anotar una perspectiva que se adecue absolutamente a estos sistemas, sea mediante la transformación de métodos, técnicas y procedimientos de la auditoria tradicional, ósea mediante la creación de unos nuevos.

A principios de los años 80's, se empiezan a utilizar técnicas de tratamiento de la información por medio de computadores, como apoyo a la labor de los auditores. El auditor de sistemas de información empieza a ser también experto en el uso de lenguajes informáticos que le sirven para escribir, compilar y ejecutar programas para la consecución de pruebas y obtención de evidencia.

Con la introducción de nuevas tecnologías, pronto se detectaron las limitaciones de los métodos tradicionales para realizar la auditoria de sistemas. En su afán de maximizar la eficiencia de los procesos de auditorias, surgen nuevos modelos que se adecuan a las crecientes necesidades del sector de las tecnologías de la información, entre ellos se tienen:

Directrices gerenciales de COBIT, desarrollado por la *Information Systems Audit Control Associatio*n (ISACA):

Las Directrices Gerenciales son un marco internacional de referencias que abordan las mejores prácticas de auditoría y control de sistemas de información. Permiten que la gerencia incluya, comprenda y controle los riesgos relacionados con la tecnología de información y establezca el enlace entre los procesos de administración, aspectos técnicos, la necesidad de controles y los riesgos asociados.

The Management of the Control of Data Information Technology, desarrollado por el Instituto Canadiense de Contadores Certificados (CICA):

Este modelo esta basado en el concepto de errores que establece responsabilidades relacionadas con la seguridad y los controles correspondientes. Dichos roles están clasificados con base en siete grupos: administración general, gerentes de sistemas, dueños, agentes, usuarios de sistemas de información, así como proveedores de servicios, desarrollo y operaciones de servicios y soporte de sistemas. Además, hace distinción entre los conceptos de autoridad, responsabilidad y respecto a control y riesgo previo al establecimiento del control, en términos de objetivos, estándares y técnicas mínimas a considerar.

SysTrust – Principios y criterios de confiabilidad de Sistemas, desarrollados por la Asociación de Contadores Públicos (AICPA) y el CICA:

Este servicio pretende incrementar la confianza de alta gerencia, clientes y socios, con respecto a la confiabilidad en los sistemas por una empresa o actividad en particular. Este modelo incluye elementos como: infraestructura, software de cualquier naturaleza, personal especializado y usuarios, procesos manuales y automatizados, y datos. El modelo persigue determinar si el sistema de información es confiable, (i.e. si un sistema funciona sin errores significativos, o fallas durante un periodo de prueba determinado bajo un ambiente dado).

Modelo de Evaluación de Capacidades de software (CMM), desarrollado por el Instituto de Ingenieros de Software (SEI):

Este modelo hace posible evaluar las capacidades o habilidades para ejecutar, de una organización con respecto al desarrollo y mantenimiento de sistemas de información. Consiste en 18 sectores clave, agrupados alrededor de cinco niveles de madurez. Se puede considerar que CMM es la base de los principios de evaluación recomendados por COBIT, así como para algunos de los procesos de administración de COBIT.

ISO/IEC 27001(*Information Technology – Security Techniques – Information Security Management System – Requirements*)

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Según el conocido “Ciclo de Deming”: PDCA – acrónimo de plan, *Do Check, Act* (Planificar, Hace, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/17799 (Actual ISO ICE 27002) y tiene su origen en la revisión de la norma Británica *British Standard* BS 7799 – 2: 2002.

Si se revisan los antecedentes de proyectos relacionados con auditoría de sistemas en la Universidad de Nariño se encuentran:
Proyecto: DEFINICION DE POLITICAS DE SEGURIDAD INFORMATICA PARA EL CENTRO DE INFORMATICA DE LA UNIVERSIDAD DE NARIÑO.

Realizado por María Constanza Torres B. y Efraín Fajardo Guevara, el trabajo consistió en realizar los procesos de auditoría a la seguridad del centro de informática de la Universidad de Nariño.

1.2. ASPECTOS GENERALES SOBRE AUDITORIA

Inicialmente se puede definir a la auditoria, como el proceso sistemático mediante el cual se obtiene y evalúa una serie de evidencias emanadas de cualquier entidad y de sus actividades, sin importar de que tipo sean, esto con el fin de determinar el grado de correspondencia del contenido informativo con las evidencias recolectadas, debe ser un proceso objetivo y limpio desligado de cualquier interés, este proceso medidor y evaluador debe ayudar a determinar, con conocimiento y certeza razonable, la calidad de los procesos, el cumplimiento de normatividades, la eficiencia en la administración de los recursos, la eficacia con la que se logran los resultados de las estrategias planteadas, entre otros.

La auditoria es un proceso sistemático por que se construye con un conjunto de fases y/o actividades que se relacionan entre ellas, con el fin de lograr un objetivo especifico; esto con apego a las normas, objetivos y principios que regulan la auditoria.

En forma sencilla y clara escribe Holmes:

"... la auditoria es el examen de las demostraciones y registros administrativos. El auditor observa la exactitud, integridad y autenticidad de tales demostraciones, registros y documentos.".[2]

Se debe tener en claro que no se puede restringir a la auditoria a eventos solamente de carácter económico, ya que la labor de la auditoria es mucho mas amplia, por lo que se pueden abarcar aspectos administrativos, manejo de recursos humanos, técnicos y demás, esto hace que la auditoria sea la herramienta de control mas completa y mas fundamentada.

Por lo tanto la auditoria se convierte en la herramienta más eficaz para aplicar una supervisión y un control, que contribuye a la creación de una cultura de disciplina en la organización, además permite descubrir a tiempo fallas en la estructura o puntos débiles existentes a nivel especifico o general.

La auditoria como función de control debe ser la herramienta a utilizar para ayudar a los Funcionarios que tienen responsabilidad administrativa, técnica y operacional a que no incurran en falta. Y es por ello que aquí el Control debe ser

[2] http://www.monografias.com/trabajos39/la-auditoria/la-auditoria.shtml.

creativo, inteligente, y constructivo de asesoramiento oportuno a todas las direcciones o gerencias a fin de que la toma de decisiones sea acertada, segura y se logren los objetivos, con la máxima eficiencia.

La responsabilidad de un procedimiento de auditoria debe ir mas allá de la búsqueda de problemas y de responsables, la visión empresarial del siglo XXI le ha impuesto mucha mas responsabilidad al proceso de auditoria, convirtiéndola en herramienta de reingeniería capaz de retroalimentar procesos o crear nuevos, la auditoria se volvió capaz de identificar necesidades, problemas y soluciones a futuro, con estas facultades el proceso de auditoria se promueve como una función permanente y a largo plazo.

El proceso que se realiza en una empresa puede ser de dos tipos con sus respectivos enfoques:

2.2.1. Auditoría interna. Es una actividad independiente que realiza la empresa y que está encaminada a la revisión de operaciones contables además de la evaluación y medición de la eficacia de otros controles, con la finalidad de prestar un servicio a la dirección. Se aplica mejor en empresas medianas que tienden a aumentar en volumen, extensión geográfica y complejidad y se hace imposible el control directo de las operaciones por parte del director.

El objetivo principal es ayudar a la dirección en el cumplimiento de sus funciones y responsabilidades, proporcionándole un análisis objetivo, evaluaciones y recomendaciones pertinentes sobre las operaciones examinadas.

Otros objetivos que se busca concretar a través de la auditoria interna son: realizar investigaciones especiales solicitadas por la dirección, preparar informes de auditoría acerca de las irregularidades que pudiesen encontrarse como resultado de las investigaciones, expresando igualmente las recomendaciones que se juzguen adecuadas, vigilar el cumplimiento de la recomendaciones contenidas en los informes emitidos con anterioridad.

La auditoria interna posee varias ventajas: facilita una ayuda primordial a la dirección al evaluar de forma relativamente independiente los sistemas de organización y de administración, facilita una evaluación global y objetiva de los problemas de la empresa que generalmente suelen ser interpretados de una manera parcial por los departamentos afectados, pone a disposición de la dirección un profundo conocimiento de las operaciones de la empresa, proporcionado por el trabajo de verificación de los datos contables y financieros, contribuye eficazmente a evitar las actividades rutinarias que generalmente se desarrollan en las grandes empresas, favorece la protección de los intereses y bienes de la empresa frente a terceros.

- **Auditoría externa.** Se puede definir como los métodos empleados por una firma externa de profesionales para averiguar la exactitud del contenido de los estados financieros presentados por una empresa. Se trata de dar carácter público, mediante la revisión, a unos estados financieros que en principio eran privados.

  Los objetivos de la auditoría externa son: proporcionar a la dirección y a los propietarios de la empresa unos estados financieros certificados por una autoridad independiente e imparcial, proporcionar asesoramiento a la gerencia y a los responsables de las distintas áreas de la empresa en materia de sistemas contables y financieros, procedimientos de organización y otras numerosas fases de la operatoria de una empresa, suministrar información objetiva que sirva de base a las entidades de información y clasificación crediticia, servir de punto de partida en las negociaciones para la compraventa de las acciones de una empresa, reducir y controlar riesgos accidentales, fraudes y otras actuaciones anormales, liberar implícitamente a la gerencia de sus responsabilidades de gestión.

  ✓ **Principios generales de la auditoría externa**

  - Exposición: Los estados financieros deben recoger por completo y con claridad todas las transacciones de la empresa.

  - Uniformidad: la base utilizada en la preparación de los estados financieros de un ejercicio no debe experimentar ninguna variación con respecto al ejercicio precedente.

  - Importancia o materialidad: Este es el criterio que debe presidir el trabajo del auditor es la importancia económica o materialidad de las partidas.

  - Moderación: De dos o más posibilidades igualmente validas se debe escoger siempre la que dé los resultados más desfavorables.

  ✓ **Normas generales de la auditoría externa:** Afectan a las condiciones que debe de reunir el auditor de y a su comportamiento en el desarrollo de la actividad de auditoría.

  - Realización por una persona competente.

  - Realización por una persona independiente.

  - Cuidado profesional en la realización del trabajo y en la confección del informe.

- ✓ **Normas de trabajo de la auditoría externa**: Hacen referencia a la preparación y ejecución del trabajo a realizar por el auditor, regulan el conjunto de técnicas de investigación e inspección aplicables a los hechos relativos a los documentos contables sujetos a examen, mediante los cuales el auditor fundamenta su opinión responsable e independiente.

  - o Programación adecuada.

  - o Supervisión adecuada.

  - o Análisis del control interno para fijar el alcance de la pruebas.

  - o Opinión basada en un material y un trabajo razonablemente suficiente.

- ✓ **Normas del informe de la auditoría externa**: Regulan los principios que han de ser observados en la elaboración y presentación del informe de auditoría estableciendo la extensión y contenido de los diferentes tipos de informes, así como los criterios que fundamenten el modelo de informe a utilizar en cada caso.

  - o Expresión de si los estados financieros se ajustan a los principios de contabilidad generalmente aceptados.

  - o Expresión de si se han presentado los estados financieros de manera uniforme con respecto al periodo precedente.

  - o Exposiciones informativas razonablemente adecuadas a los estados financieros.

  - o El informe debe contener un dictamen sobre los estados financieros considerados en su conjunto.

- ✓ **Procedimientos de la auditoría externa:** Son la serie de trabajos que hay que realizar para el adecuado cumplimiento de los principios y las normas, antes de presentar el informe definitivo. Se pueden señalar los siguientes procedimientos:

  - o Revisión de las actividades en las operaciones.

  - o Inspecciones físicas y recuentos.

  - o Obtención de pruebas de evidencia.

  - o Obtención de pruebas de exactitud.

- Preparación de reconciliaciones.

1.3. EL AUDITOR

El auditor se refiere a la persona que asume la responsabilidad de realizar un trabajo de este tipo, en todo caso el auditor debe poseer ciertas cualidades para afrontar un trabajo como este:

- El auditor debe dominar las técnicas y las metodologías que se utilizaran.
- Debe ser abierto en sus relaciones personales y debe saber dialogar.
- Debe poseer habilidades de carácter personal como independencia en el criterio, objetividad, diplomacia etc.
- El auditor debe mantener un cierto grado de independencia en los asuntos que se encuentra evaluando.
- El auditor tiene la obligación de realizar con esmero y cuidado el dictamen o informe para el que fue contratado.
- Debe poseer una actitud positiva frente a la entidad evaluada.
- Debe tener estabilidad emocional frente la entidad.
- Es su obligación la de respetar las ideas de los demás.
- Debe tener capacidad para la negociación.
- Sera discreto y respetuoso con la información de la empresa.
- Su comportamiento debe ceñirse a la ética profesional.

Dadas estas características el auditor responsablemente deberá cumplir con las siguientes funciones:

- Estudiar la normatividad, misión, objetivos, políticas, estrategias, planes y programas de trabajo
- Desarrollar el programa de trabajo de una auditoria
- Definir los objetivos, alcance y metodología para instrumentar una auditoria

- Captar la información necesaria para evaluar la funcionalidad y efectividad de los procesos, funciones y sistemas utilizados

- Recabar y revisar estadísticas sobre volúmenes y cargas de trabajo

- Diagnosticar sobre los métodos de operación y los sistemas de información

- Detectar los hallazgos y evidencias e incorporarlos a los papeles de trabajo

- Respetar las normas de actuación dictadas por los grupos de filiación, corporativos, sectoriales e instancias normativas y, en su caso, globalizadoras

- Proponer los sistemas administrativos y/o las modificaciones que permitan elevar la efectividad de la organización

- Analizar la estructura y funcionamiento de la organización en todos sus ámbitos y niveles

- Revisar el flujo de datos y formas

- Considerar las variables ambientales y económicas que inciden en el funcionamiento de la organización

- Analizar la distribución del espacio y el empleo de equipos de oficina

- Evaluar los registros contables e información financiera

- Mantener el nivel de actuación a través de una interacción y revisión continua de avances

- Proponer los elementos de tecnología de punta requeridos para impulsar el cambio organizacional

- Diseñar y preparar los reportes de avance e informes de una auditoria

1.4. TIPOS DE AUDITORIA

Existen algunos tipos de Auditoría entre los que la Auditoría de Sistemas integra un mundo paralelo pero diferente y peculiar resaltando su enfoque a la función informática.

Entre los principales enfoques de Auditoría tenemos los siguientes:

1.4.1. Auditoría fiscal. Es una comprobación científica y sistemática de los estados financieros, libros de cuentas, comprobantes y otros registros financieros y legales de una persona natural, firma o corporación realizado por un auditor con el fin de asegurar si los libros han sido llevados por los principios de contabilidad generalmente aceptados y así brindar confianza y credibilidad a las personas, ya sean naturales o jurídicas que puedan estar interesadas en los estados de la empresa. La persona quien realice la auditoría debe ser un ente ajeno a la empresa, de esta manera se evitan vínculos que puedan verse reflejados en una opinión positiva o parcialización a través de la empresa sin que la misma lo merezca. También es necesario mencionar que si la auditoría esta hecha por una firma con una amplia y reconocida trayectoria esta otorgara una mayor credibilidad y confianza a las personas interesadas. En conclusión la auditoría fiscal se dedica a observar el cumplimiento de las leyes fiscales.

La auditoría fiscal tiene como principales objetivos:

- Determinar si sus sistemas contables son aceptables
- Conocer si el catálogo de cuentas es aceptable
- Verificar si se está al día en el cumplimiento de sus deberes formales
- Detectar áreas de riesgo y saber exactamente que correctivos aplicar

1.4.2. Auditoría financiera. Es una revisión de los estados financieros similar a la auditoría externa. Su objetivo es expresar una opinión sobre si las cifras del balance y la cuenta de resultados presentan razonablemente la situación actual de la empresa de acuerdo con los principios de contabilidad generalmente aceptados.

En general la auditoría financiera busca comprobar la veracidad de los estados financieros de la empresa y preparar informes de acuerdo a principios contables

1.4.3. Auditoria operacional. Es una evaluación objetiva, constructiva, sistemática y profesional de las actividades relativas al proceso de gestión de una organización, con el fin de determinar el grado de eficiencia, eficacia, efectividad, economía, equidad, excelencia y valoración de costos ambientales, con que son manejados los recursos; la adecuación y fiabilidad de los sistemas de información y control, de manera que cumpla con las políticas establecidas para alcanzar sus objetivos.

Los informes emergentes de este tipo de auditoría son:

- Auditoría Operativa, relacionada básicamente con los objetivo de eficacia, eficiencia y economía.

- Evaluaciones del Sistema de Control Interno, cuyo propósito es evaluar el diseño y funcionamiento de los Sistemas establecidos.

La auditoría operativa implica:

- El período objeto de examen

- Examen y verificación de la información relativa al desempeño institucional

- Revisión y elaboración de informes sobre la administración de recursos

- Análisis de actividades y procesos clave, evaluación de sistemas de información y control

- Verificar la utilización de recursos públicos de conformidad a principios de eficiencia, efectividad, economía, eficacia, equidad y excelencia

- Verificar el cumplimiento de metas y objetivos

- Evaluar la gestión

Este tipo de auditoria se aplica generalmente en el Sector Público, Sector Privado, Sector Social.

El objetivo primordial de la auditoria operacional es brindar a todo tipo de organización la información necesaria para utilizar esta poderosa herramienta en forma congruente con sus necesidades y capacidad instalada, a fin de evaluar su comportamiento y derivar las medidas requeridas para mejorar su desempeño. Otras razones por las que se realiza esta auditoria son para establecer el grado en que la entidad y sus servidores han cumplido adecuadamente los deberes y atribuciones que les han sido asignados, determinar el grado en que el organismo y sus funcionarios controlan y evalúan la calidad tanto en los servicios que presta como en los bienes adquiridos y verificar que la entidad auditada cumpla con normas y demás disposiciones.

1.4.4. Auditoria administrativa. Independientemente de ser ella misma parte integrante del sistema total de control superior, es la principal herramienta para la revisión y evaluación de los resultados logrados. Cumple con una doble misión: primero, como parte integrante del control superior; es decir, un medio para

obtener y mantener el control; el segundo es; el medio principal para la medición y evaluación de resultados.

Por tanto la dirección superior, propietarios, accionistas, auditores financieros y otros interesados deben confiar en ésta para la prevención de inconvenientes, y para garantizar la adecuada marcha del sistema.

La auditoria administrativa, como función interna, puede verse desde el punto de vista de la organización como:

- Una extensión de la auditoria interna financiera
- Función independiente de la administración financiera
- Forma departamental con la auditoria interna
- Órgano asesor del consejo de administración

Las funciones de a auditoria administrativa deben quedar enmarcadas dentro de la organización de una empresa en una unidad que, por su situación jerárquica le permita la consecución de sus fines.

El nivel donde deberá quedar la unidad departamental de auditoría administrativa reunirá las siguientes características:

- Jerarquía suficiente para poder inmiscuirse en cualquier unidad administrativa de la empresa
- Que el tipo de funciones de dicha unidad sea relacionado con la dirección, control y coordinación
- Que tenga suficiente autoridad sobre los demás departamentos

Funciones que se van a desarrollar en una auditoria administrativa:

- Investigación constante de planes y objetivos
- Estudio de las políticas y sus prácticas
- Revisión constante de la estructura orgánica
- Estudio constante de las operaciones de la empresa
- Analizar la eficiencia de la utilización de recursos humanos y materiales

- Revisión del equilibrio de las cargas de trabajo

- Revisión constante de los métodos de control

1.4.5. Auditoria integral. Es el proceso de obtener y evaluar objetivamente, en un período determinado, evidencia relativa a la información financiera, al comportamiento económico y al manejo de una entidad con la finalidad de informar sobre el grado de correspondencia entre aquellos y los criterios o indicadores establecidos o los comportamientos generalizados.

El objetivo de la auditoria integral es evaluar los sistemas de control, implantados por la Gerencia General que le permitan medir el rendimiento económico y los recursos financieros de la empresa.

Además con la auditoria integral se pretende conocer la normativa que regula a la auditoría Integral, analizar el ambiente de aplicación de la auditoría Integral, verificar a través de la utilización de un conjunto estructurado de proceso tomando como objetivo la evaluación sistemática y permanente del ente económico para una aseveración verificable.

La Auditoría Integral implica la ejecución de un trabajo con el trabajo o enfoque, por analogía de las revisiones financieras, de cumplimiento, control interno y de gestión, sistema y medio ambiente con los siguientes objetivos:

- Determinar, si los Estados Financieros se presentan de acuerdo con los Principios de Contabilidad Generalmente Aceptados.

- Determinar, si el ente ha cumplido, en el desarrollo de sus operaciones con las disposiciones legales que le sean aplicables, sus reglamentos, los estatutos y las decisiones de los órganos de dirección y administración.

- Evaluar la estructura del control interno del ente con el alcance necesario para dictaminar sobre el mismo.

- Evaluar el grado de eficiencia en el logro de los objetivos previstos por el ente y el grado de eficiencia y eficacia con que se han manejado los recursos disponibles.

- Evaluar los mecanismos, operaciones, procedimientos, derechos a usuarios, responsabilidad, facultades y aplicaciones específicas de control relacionadas con operaciones en computadora.

- Evaluar el impacto medioambiental producido de manera directa o indirecta por empresas que presentan un perfil ambiental diferente, condicionado por los riesgos aparentes asociados con sus procesos y productos; la edad, historia y estado de una planta, el marco jurídico en el cual opera.

Los principios generales de auditoria integral son: independencia, objetividad, permanencia, certificación, integridad, planeamiento, supervisión, oportunidad, forma, cumplimiento de las Normas de Profesión.

Para que el ejercicio de la Auditoría Integral se desarrolle en un ambiente controlado, es importante conducirla dentro de un concepto de normas que provean una estructura, como la posibilidad de pronosticar los resultados.

La aplicación de normas ayudará a desarrollar una auditoría de alta calidad respondiendo a la necesidad de completar tareas difíciles en forma oportuna, evitando formar juicios prematuros basados en información incompleta por la falta de tiempo, asimismo, establecen orden y disciplina, produciendo auditorías efectivas, garantizando la veracidad de los hallazgos y el soporte adecuado para las recomendaciones, consecuentemente habrá una mayor aceptación por parte de la gerencia.

1.4.6. Auditoria de sistemas. Se ocupa de analizar la actividad que se conoce como técnica de sistemas en todas sus facetas. Hoy, la importancia creciente de las telecomunicaciones ha propiciado que las comunicaciones. Líneas y redes de las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de sistemas.

Su finalidad es el examen y análisis de los procedimientos administrativos y de los sistemas de control interno de la compañía auditada. Al finalizar el trabajo realizado, los auditores exponen en su informe aquellos puntos débiles que hayan podido detectar, así como las recomendaciones sobre los cambios convenientes a introducir, en su opinión, en la organización de la compañía.

Normalmente, las empresas funcionan con políticas generales, pero hay procedimientos y métodos, que son términos más operativos. Los procedimientos son también sistemas; si están bien hechos, la empresa funcionará mejor. La auditoría de sistemas analiza todos los procedimientos y métodos de la empresa con la intención de mejorar su eficacia.

Existen varios campos de acción en los que la auditoria informática de sistemas puede operar entre ellos se tienen las auditorias más destacadas del tipo:

- **Sistemas operativos.** Engloba los Subsistemas de Teleprocesos, Entrada/Salida, etc. Debe verificarse en primer lugar que los Sistemas están actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera. El análisis de las versiones de los Sistemas Operativos permite descubrir la posible incompatibilidad entre otros productos de Software Básicos adquiridos por la instalación y determinadas versiones de aquellas. Deben revisarse los parámetros variables de las librerías más importantes de los Sistemas, por si difieren de los valores habituales aconsejados por el constructor.

- **Software básico.** Es fundamental para el auditor conocer los productos de software básico que han sido facturados aparte de la propia computadora. Esto, por razones económicas y por razones de comprobación de que la computadora podría funcionar sin el producto adquirido por el cliente. En cuanto al software desarrollado por el personal informático de la empresa, el auditor debe verificar que este no agreda ni condiciona al Sistema Igualmente, debe considerar el esfuerzo en términos de costes, por si hubiera alternativas más económicas.

  La auditoría, al igual que cualquier otra actividad, requiere de una buena planeación, que le permita desarrollarse eficientemente y oportunamente.

- **Auditoria web.** La auditoría web está diseñada para identificar cuáles son los puntos débiles de la presencia online, para mejorarla y para que en los puntos fuertes se pueda sacar el máximo rendimiento a la internet

  Con los diferentes tipos de auditoria web se podrá conocer:

  - ✓ Las limitaciones técnicas de la página
  - ✓ Que le falta a la página para estar optimizada
  - ✓ Quién y desde dónde vienen las visitas
  - ✓ Cómo se mueven los usuarios de la página
  - ✓ Qué productos o servicios visitan más los usuarios
  - ✓ Qué sitios enlazan la página
  - ✓ Con que palabras clave está mejor posicionada la pagina

1.5. AUDITORIA DE SISTEMAS COMO OBJETO DE ESTUDIO

Desde hace varios años, motivados por el espectacular avance de los sistemas dentro de las organizaciones, surgió la necesidad de evaluar no solo los sistemas, sino también la información, sus componentes y todo lo relacionados con dichos sistemas informáticos, a lo que se le denominó auditoria de sistemas.

"La auditoria de sistemas es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. También permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es critica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes".[3]

La auditoria de sistemas permite además verificar que la información desde su entrada, procedimientos, controles, almacenamientos y salidas, sea integra y verificable y por tanto permita el apoyo a la toma de decisiones dentro de una organización

Dentro de este procedimiento es necesario evaluar los mecanismos de control implantados en una organización, determinando así, si son adecuados y cumplen con los objetivos o estrategias, de esta manera, es posible proponer cambios que se deberían realizar para el mejoramiento de los mismos. Estos mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia. [4]

1.5.1. Alcance de la auditoria de sistemas. Dentro del alcance de una auditoria de sistemas, es necesario determinar con precisión el entorno y los límites en que va a desarrollarse la auditoria de sistemas. La indefinición de los alcances de la auditoria compromete el éxito o el fracaso de la misma. Así mismo, las personas que realizan la auditoría han de conocer con la mayor exactitud posible los objetivos a los que su tarea debe llegar.

[3] http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica
[4] http://rie.cl/?a=31081

1.5.2. Objetivos de la auditoria de sistemas

- **Objetivo general de la auditoria de sistemas.** El objetivo principal de la auditoria de sistemas es evaluar el uso adecuado de los sistemas para el correcto ingreso de datos, el procesamiento adecuado de la información y la emisión oportuna de los resultados en la organización, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas de información dentro de la empresa.[5]

- **Objetivos específicos de la auditoria de sistemas**

  ✓ El control de la función informática

  ✓ El análisis de la eficiencia de los Sistemas Informáticos

  ✓ La verificación del cumplimiento de la Normativa en este ámbito

  ✓ La revisión de la eficaz gestión de los recursos informáticos.

  La auditoria de sistemas sirve para mejorar ciertas características en la empresa como:

  ✓ Eficiencia

  ✓ Eficacia

  ✓ Rentabilidad

  ✓ Seguridad

1.5.3. Principales pruebas y herramientas para efectuar una auditoría de sistemas.

- **Pruebas sustantivas:** Estas pruebas permiten evaluar el grado de confiabilidad del sistema de información de la organización. Para esto se realiza una verificación por medio de observación, cálculos, muestreos, entrevistas, exámenes analíticos, revisiones y conciliaciones. evalúan de la misma manera la exactitud, integridad y validez de la información.

[5] http://www.monografias.com/trabajos5/audi/audi.shtml

- **Pruebas de cumplimiento:** Estas pretenden evaluar y verifican el grado de cumplimiento de aquello extraído el análisis de la muestra. Permite evidenciar los controles existentes y que son aplicables efectiva y uniformemente.

  Las principales herramientas de las que dispone un auditor informático son:

  ✓ Observación

  ✓ Realización de cuestionarios

  ✓ Entrevistas a auditados y no auditados

  ✓ Muestreo estadístico

  ✓ Flujogramas

  ✓ Listas de chequeo

  ✓ Mapas conceptuales

1.5.4. Perfiles profesionales de los auditores informáticos.

Tabla 1: Perfiles Profesionales y Actividades

Profesión	**Actividades y conocimientos deseables**
Informático Generalista	Con experiencia amplia en ramas distintas. Deseable que su labor se haya desarrollado en Explotación y en Desarrollo de Proyectos. Conocedor de Sistemas.
Experto en Desarrollo de Proyectos	Amplia experiencia como responsable de proyectos. Experto analista. Conocedor de las metodologías de Desarrollo más importantes.
Técnico de Sistemas	Experto en Sistemas Operativos y Software Básico. Conocedor de los productos equivalentes en el mercado. Amplios conocimientos de Explotación.

Tabla 2: Perfiles Profesionales y Actividades (continuación)

Experto en Bases de Datos y Administración de las mismas.	Con experiencia en el mantenimiento de Bases de Datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación
Experto en Software de Comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Muy experto en Subsistemas de teleproceso.
Experto en Explotación y Gestión de CPD´S	Responsable de algún Centro de Cálculo. Amplia experiencia en Automatización de trabajos. Experto en relaciones humanas. Buenos conocimientos de los sistemas.
Técnico de Organización	Experto organizador y coordinador. Especialista en el análisis de flujos de información.
Técnico de evaluación de Costes	Economista con conocimiento de Informática. Gestión de costes.

1.5.5. Pasos a seguir para una auditoria de sistemas en una organización.

- **Estudio preliminar.** Para realizar dicho estudio se examinan las funciones y actividades generales del área o departamento de sistemas, con el fin de tener un contacto inicial con el personal de dicha área, y conocer a grandes rasgos la distribución del sistema, características de equipos, instalaciones y medidas de seguridad visibles.

  Para su realización el auditor debe conocer lo siguiente:

  - ✓ **Organización:** Es de vital importancia conocer dentro del departamento o área de sistemas quien es el jefe, quien diseña y quien ejecuta, para lo cual es necesario conocer:

    - o Organigrama: El organigrama permite conocer la estructura oficial dentro de la organización a auditar.

    - o Departamentos: Es importante conocer los departamentos que hacen parte de la organización y las funciones que se deben llevar a cabo dentro de cada uno de ellos.

- Relaciones Jerárquicas y funcionales entre órganos de la Organización: Es necesario verificar si dentro de la organización se cumplen las relaciones funcionales y jerárquicas que se evidencian dentro del organigrama.

✓ **Corrientes de información:** Los flujos de información entre los diferentes departamentos dentro de una organización son de vital importancia ya que evidencian una gestión eficiente, siempre y cuando estas corrientes no vayan en direcciones no contempladas dentro del organigrama.

En muchas ocasiones es posible que se hayan creado canales de información alternativos, lo cual ocurre cuando existen pequeños o grandes fallos en la estructura de la organización.

Además, la aparición de corrientes de información no planeados pueden obedecer a afinidades personales o desacato a las reglas establecidas. Los cuales pueden producir perturbaciones dentro de la organización.

✓ **Flujos de información:** Dentro del proceso de auditoria es necesario verificar que los nombres de los cargos dentro de la organización correspondan a las funciones que realiza esa persona.

Puede ocurrir que bajo nombres de cargos diferentes se realicen funciones idénticas, en este caso se estaría realizando tareas redundantes lo cual podría conllevar a deficiencias estructurales.

✓ **Entorno operacional:** Es importante conocer por parte de los auditores de sistemas la referencia del entorno en el cual se va a trabajar, esto se logra determinando:

- Ubicación geográfica del o los centros de procesamiento de información de la empresa. Evaluando además el personal responsable de cada uno de ellos.

- Arquitectura y configuración de Hardware y Software: es fundamental la verificación de la compatibilidad e intercomunicación de los equipos ya que estas, están estrechamente ligadas a los grados de seguridad lógica de las organizaciones.

- Situación geográfica de los Sistemas: el equipo auditor debe estudiar la información que proporcione la organización sobre los elementos físicos y lógicos de las instalaciones.

- Comunicación y Redes de Comunicación: se debe disponer de un inventario, estado y características de las redes de comunicación.

- ✓ **Aplicaciones bases de datos:** Finalmente para el equipo auditor es necesario tener una idea general de los procesos informáticos realizados dentro de la organización.

  Para ello es necesario recolectar la siguiente información:

  - o Inventario de Hardware y Software

  - o Volumen, antigüedad y complejidad de las Aplicaciones

  Se clasificará globalmente la existencia total o parcial de metodología en el desarrollo de las aplicaciones.

  Si se han utilizados varias a lo largo del tiempo se pondrá de manifiesto:

  - o Metodología del diseño: La existencia de una adecuada documentación de las aplicaciones proporciona beneficios tangibles e inmediatos muy importantes.

  La documentación de programas disminuye gravemente el mantenimiento de los mismos.

  - o Documentación: El auditor recaudara información de tamaño y características de las Bases de Datos, clasificándolas en relación y jerarquías. Hallará un promedio de número de accesos a ellas por hora o días. Esta operación se repetirá con los ficheros, así como la frecuencia de actualizaciones de los mismos.

  Estos datos proporcionan una visión aceptable de las características de la carga informática.

- **Determinación de recursos de la auditoría de sistemas.** Por medio de los resultados del estudio preliminar es posible determinar los recursos humanos y físicos que son necesarios en el proceso de auditoría.

- **Elaboración del plan y de los programas de trabajo.** El plan de trabajo se realiza de acuerdo a los siguientes criterios:

  - ✓ El proceso de auditoría se llevara a cabo en áreas generales o específicas.

  - ✓ La auditoria se hará de manera global o especifica.

- ✓ De acuerdo a si se manejaran recursos genéricos o específicos se realizará un cronograma de trabajo.

- ✓ El Plan establece disponibilidad futura de los recursos durante la revisión.

- ✓ El Plan estructura las tareas a realizar por cada integrante del grupo auditoria.

- ✓ En el Plan se expresan todas las ayudas que el auditor ha de recibir del auditado.

Una vez elaborado el Plan, se procede a la Programación de actividades, esta ha de ser lo suficientemente flexible como para permitir modificaciones a lo largo del proyecto.

- **Actividades de la auditoría de sistemas.** La auditoría de sistemas general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos.

  Cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se obtiene más rápidamente y con menor calidad.

  - ✓ **Técnicas de trabajo:**

    - o Análisis de la información recabada del auditado

    - o Análisis de la información propia

    - o Cruzamiento de las informaciones anteriores

    - o Entrevistas

    - o Simulación

    - o Muestreos

  - ✓ **Herramientas:**

    - o Cuestionario general inicial

    - o Cuestionario Checklist

    - o Estándares

- Monitores
- Simuladores (Generadores de datos)
- Paquetes de auditoría (Generadores de Programas)
- Matrices de riesgo

✓ **Informe final.** El informe final de la auditoria de sistemas se realiza por escrito, el cual contempla la siguiente estructura:

- Definición de objetivos y alcance de la auditoría
- Enumeración de temas objeto de la auditoria
- Cuerpo de la auditoria: para lo cual se mostrara para cada tema lo siguiente:
  - Situación actual
  - Tendencias futuras
  - Puntos débiles y amenazas
  - Recomendaciones y planes de acción
  - Redacción posterior de la Carta de Introducción o Presentación

1.6. METODOLOGÍAS DE AUDITORIA DE SISTEMAS

La auditoria de sistemas en el ámbito empresarial, ha sido de gran importancia, puesto que con ella se pretende gestionar la información y sirve como apoyo a la toma de decisiones. Además se busca disponer de un sistema de información que sea eficiente y eficaz para obtener la mayor productividad y calidad posibles, debido a que la información se ha convertido en el activo más importante de las empresas.

En la actualidad, gran parte de las organizaciones consideran que la información y la tecnología representan activos importantes para la misma, sin dejar de lado otros activos indispensables, como los requerimientos de calidad, controles, seguridad e información. Por tal razón los directivos deben establecer un adecuado sistema de control interno, para proporcionar seguridad razonable, respecto a si están lográndose los objetivos como: promover la efectividad y eficiencia de las operaciones, proteger y conservar todos los recursos de la organización, cumplir las leyes y reglamentos internos y externos relacionados con la empresa.

Para esto, se hace necesario aplicar una auditoria de sistemas llevando a cabo una metodología adecuada, que permita evaluar de manera objetiva las vulnerabilidades o falta de controles existentes en la empresa.

Las metodologías desarrolladas y utilizadas en la auditoría y el control informático, se dividen en dos grupos:

- Cuantitativas

- Cualitativas

Las metodologías cuantitativas están basadas en un modelo matemático, diseñadas para producir una lista de riesgos que pueden compararse entre sí con facilidad por tener asignados unos valores numéricos. Estos valores son datos de probabilidad de ocurrencia de un evento que se debe extraer de un riesgo de incidencias donde el número de incidencias tiende al infinito.

Y las metodologías cualitativas están basadas en el criterio humano capaz de definir un proceso de trabajo. Así mismo, esta metodología establece métodos estadísticos y lógica borrosa, que requiere menos recursos humanos y menos tiempo que las metodologías cuantitativas.

Esta metodología presenta un enfoque amplio y logra un plan de trabajo flexible y reactivo. Sin embargo tiene la desventaja de depender mucho de la experiencia,

habilidad y calidad del profesional involucrado. Dicha anomalía nace de la dificultad que tiene un profesional sin experiencia que asume la función auditora y busca una fórmula fácil que le permita empezar su trabajo rápidamente. Por lo tanto es necesario que el auditor tenga una gran experiencia y una gran formación tanto auditora como informática. Esta formación debe ser adquirida mediante el estudio y la práctica. [6]

En la auditoria de sistemas existen varias metodologías como: COBIT (ISACA), COSO, SAC, AICPA (SAS), IFAC (NIA), MARGERIT y EDP[7]. Sin embargo, las metodologías más utilizadas son: COBIT y COSO.

Estas últimas hacen parte de los modelos a seguir dentro del control interno y son necesarias para desarrollar cualquier proyecto de manera ordenada y eficaz, por lo que cada una cumple un papel importante y al optar por una de ellas, el auditor debe cumplirlas a cabalidad.

1.6.1. COBIT (Control Objectives for Information and related Technology). La Organización ISACA (Information Systems Audit and Control Association), se formo como una fundación de educación para llevar a cabo los esfuerzos de investigación a gran escala para expandir el conocimiento y el valor de la gobernanza de las Tecnologías de Información (TI) y el campo de control. A través de su Fundación, publicó en 1995 el COBIT, como resultado de cuatro años de intensa investigación [8].

El COBIT es una metodología utilizada en las empresas para auditar los sistemas de información, donde se evalúa la gestión y el control, enfocado a los administradores de las TI, los usuarios y los auditores encargados del proceso.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos, esta basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

La estructura del modelo COBIT evalúa los criterios de información, como la seguridad y calidad, así como también se verifican los recursos que comprenden la tecnología de información, como el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos implicados en la organización.

---

[6] PIATTINI, Mario y Emilio del Peso. Auditoría Informática. Un enfoque práctico. Editorial RA-MA.

[7] Tesis, Auditoria al modulo de historia clínica. Jenny Burgos y Carolina Domínguez. Año 2007. Pág. 59-60 y 87-94.

[8] http://www.degerencia.com/articulos/los_cinco_componentes_del_control_interno.

Cuando se implementa el COBIT adecuadamente en una organización, se evalúa de manera ágil y consistente el cumplimiento de los objetivos de control, haciendo que los procesos y recursos de información y tecnología contribuyan al logro de los objetivos de la empresa.

El modelo COBIT, clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro dominios:

- **Dominio: Planificación y organización (PO).** Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos de negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

  ✓ **Procesos:**

  - **PO1 Definición de un plan Estratégico**

    - PO1.1 Administración del Valor de TI
    - PO1.2 Alineación de TI con el Negocio
    - PO1.3 Evaluación del Desempeño y la Capacidad Actual
    - PO1.4 Plan Estratégico de TI
    - PO1.5 Planes Tácticos de TI
    - PO1.6 Administración del Portafolio de TI

    Objetivo: Lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, para asegurar sus logros futuros.

    Su realización se concreta a través un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo, los que deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo, teniendo en cuenta:

    - La definición de objetivos de negocio y necesidades de TI, la alta gerencia será la responsable de desarrollar e implementar planes a largo y corto plazo que satisfagan la misión y las metas generales de la organización.

- El inventario de soluciones tecnológicas e infraestructura actual, se deberá evaluar los sistemas existentes en términos de: nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, costo y fortalezas y debilidades, con el propósito de determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes.

- Los cambios organizacionales, se deberá asegurar que se establezca un proceso para modificar oportunamente y con precisión el plan a largo plazo de tecnología de información con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de la TI

- Estudios de factibilidad oportunos, para que se puedan obtener resultados efectivos

o **PO2 Definición de la Arquitectura de Información**

- PO2.1 Modelo de Arquitectura de Información Empresarial

- PO2.2 Diccionario de Datos Empresarial y Reglas de Sintaxis de Datos

- PO2.3 Esquema de Clasificación de Datos

- PO2.4 Administración de Integridad

Objetivo: Satisfacer los requerimientos de negocio, organizando de la mejor manera posible los sistemas de información, a través de la creación y mantenimiento de un modelo de información de negocio, asegurándose que se definan los sistemas apropiados para optimizar la utilización de esta información, tomando en consideración:

- La documentación deberá conservar consistencia con las necesidades permitiendo a los responsables llevar a cabo sus tareas eficiente y oportunamente.

- El diccionario de datos, el cual incorporara las reglas de sintaxis de datos de la organización y deberá ser continuamente actualizado.

- La propiedad de la información y la clasificación de severidad con el que se establecerá un marco de referencia de clasificación general relativo a la ubicación de datos en clases de información.

o **PO3 Determinación de la dirección tecnológica**

- PO3.1 Planeación de la Dirección Tecnológica
- PO3.2 Plan de Infraestructura Tecnológica
- PO3.3 Monitoreo de Tendencias y Regulaciones Futuras
- PO3.4 Estándares Tecnológicos
- PO3.5 Consejo de Arquitectura de TI

Objetivo: Aprovechar al máximo de la tecnología disponible o tecnología emergente, satisfaciendo los requerimientos de negocio, a través de la creación y mantenimiento de un plan de infraestructura tecnológica, tomando en consideración:

- La capacidad de adecuación y evolución de la infraestructura actual, que deberá concordar con los planes a largo y corto plazo de tecnología de información y debiendo abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.
- El monitoreo de desarrollos tecnológicos que serán tomados en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.
- Las contingencias (por ejemplo, redundancia, resistencia, capacidad de adecuación y evolución de la infraestructura), con lo que se evaluará sistemáticamente el plan de infraestructura tecnológica.
- Planes de adquisición, los cuales deberán reflejar las necesidades identificadas en el plan de infraestructura tecnológica.

o **PO4 Definición de la organización y de las relaciones de TI**

- PO4.1 Marco de Trabajo de Procesos de TI
- PO4.2 Comité Estratégico de TI
- PO4.3 Comité Directivo de TI
- PO4.4 Ubicación Organizacional de la Función de TI
- PO4.5 Estructura Organizacional
- PO4.6 Establecimiento de Roles y Responsabilidades

- PO4.7 Responsabilidad de Aseguramiento de Calidad de TI
- PO4.8 Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento
- PO4.9 Propiedad de Datos y de Sistemas
- PO4.10 Supervisión
- PO4.11 Segregación de Funciones
- PO4.12 Personal de TI
- PO4.13 Personal Clave de TI
- PO4.14 Políticas y Procedimientos para Personal Contratado
- PO4.15 Relaciones

Objetivo: Prestación de servicios de TI

Esto se realiza por medio de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas, teniendo en cuenta:

- El comité de dirección el cual se encargara de vigilar la función de servicios de información y sus actividades.
- Propiedad, custodia, la Gerencia deberá crear una estructura para designar formalmente a los propietarios y custodios de los datos. Sus funciones y responsabilidades deberán estar claramente definidas.
- Supervisión, para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente
- Segregación de funciones, con la que se evitará la posibilidad de que un solo individuo resuelva un proceso crítico.
- Los roles y responsabilidades, la gerencia deberá asegurarse de que todo el personal deberá conocer y contar con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas
- La descripción de puestos, deberá delinear claramente tanto la responsabilidad como la autoridad, incluyendo las definiciones de las

habilidades y la experiencia necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.

- Los niveles de asignación de personal, deberán hacerse evaluaciones de requerimientos regularmente para asegurar para asegurar una asignación de personal adecuada en el presente y en el futuro.

- El personal clave, la gerencia deberá definir e identificar al personal clave de tecnología de información.

- **PO5 Manejo de la inversión**

  - PO5.1 Marco de Trabajo para la Administración Financiera

  - PO5.2 Prioridades Dentro del Presupuesto de TI

  - PO5.3 Proceso Presupuestal

  - PO5.4 Administración de Costos de TI

  - PO5.5 Administración de Beneficios

  Objetivo: tiene como finalidad la satisfacción de los requerimientos de negocio, asegurando el financiamiento y el control de desembolsos de recursos financieros.

  Su realización se concreta a través presupuestos periódicos sobre inversiones y operaciones establecidas y aprobados por el negocio, teniendo en cuenta:

  - Las alternativas de financiamiento, se deberán investigar diferentes alternativas de financiamiento.

  - El control del gasto real, se deberá tomar como base el sistema de contabilidad de la organización, mismo que deberá registrar, procesar y reportar rutinariamente los costos asociados con las actividades de la función de servicios de información

  - La justificación de costos y beneficios, deberá establecerse un control gerencial que garantice que la prestación de servicios por parte de la función de servicios de información se justifique en cuanto a costos. Los beneficios derivados de las actividades de TI deberán ser analizados en forma similar.

- **PO6 Comunicación de la dirección y aspiraciones de la gerencia**

- PO6.1 Ambiente de Políticas y de Control
- PO6.2 Riesgo Corporativo y Marco de Referencia de Control Interno de TI
- PO6.3 Administración de Políticas para TI
- PO6.4 Implantación de Políticas de TI
- PO6.5 Comunicación de los Objetivos y la Dirección de TI

Objetivo: Asegura el conocimiento y comprensión de los usuarios sobre las aspiraciones del alto nivel (gerencia), se concreta a través de políticas establecidas y transmitidas a la comunidad de usuarios, necesitándose para esto estándares para traducir las opciones estratégicas en reglas de usuario prácticas y utilizables. Toma en cuenta:

- Los código de ética / conducta, el cumplimiento de las reglas de ética, conducta, seguridad y estándares de control interno deberá ser establecido por la Alta Gerencia y promoverse a través del ejemplo.
- Las directrices tecnológicas
- El cumplimiento, la Gerencia deberá también asegurar y monitorear la duración de la implementación de sus políticas.
- El compromiso con la calidad, la Gerencia de la función de servicios de información deberá definir, documentar y mantener una filosofía de calidad, debiendo ser comprendidos, implementados y mantenidos por todos los niveles de la función de servicios de información.
- Las políticas de seguridad y control interno, la alta gerencia deberá asegurar que esta política de seguridad y de control interno especifique el propósito y los objetivos, la estructura gerencial, el alcance dentro de la organización, la definición y asignación de responsabilidades para su implementación a todos los niveles y la definición de multas y de acciones disciplinarias asociadas con la falta de cumplimiento de estas políticas.

o **PO7 Administración de recursos humanos**

- PO7.1 Reclutamiento y Retención del Personal
- PO7.2 Competencias del Personal

- PO7.3 Asignación de Roles
- PO7.4 Entrenamiento del Personal de TI
- PO7.5 Dependencia Sobre los Individuos
- PO7.6 Procedimientos de Investigación del Personal
- PO7.7 Evaluación del Desempeño del Empleado
- PO7.8 Cambios y Terminación de Trabajo

Objetivo: Maximizar las contribuciones del personal a los procesos de TI, satisfaciendo así los requerimientos de negocio, a través de técnicas sólidas para administración de personal, tomando en consideración:

- El reclutamiento y promoción, deberá tener como base criterios objetivos, considerando factores como la educación, la experiencia y la responsabilidad.
- Los requerimientos de calificaciones, el personal deberá estar calificado, tomando como base una educación, entrenamiento y o experiencia apropiados, según se requiera
- La capacitación, los programas de educación y entrenamiento estarán dirigidos a incrementar los niveles de habilidad técnica y administrativa del personal.
- La evaluación objetiva y medible del desempeño, se deberá asegurar que dichas evaluaciones sean llevada a cabo regularmente según los estándares establecidos y las responsabilidades específicas del puesto. Los empleados deberán recibir asesoría sobre su desempeño o su conducta cuando esto sea apropiado.

o **PO8 Asegurar el cumplimiento con los requerimientos Externos**

Objetivo: Cumplir con obligaciones legales, regulatorias y contractuales
Para ello se realiza una identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, llevando a cabo las medidas apropiadas para cumplir con ellos y se toma en consideración:

- Definición y mantenimiento de procedimientos para la revisión de requerimientos externos, para la coordinación de estas actividades y para el cumplimiento continúo de los mismos.

- Leyes, regulaciones y contratos
- Revisiones regulares en cuanto a cambios
- Búsqueda de asistencia legal y modificaciones
- Seguridad y ergonomía con respecto al ambiente de trabajo de los usuarios y el personal de la función de servicios de información.
- Privacidad
- Propiedad intelectual
- Flujo de datos externos y criptografía

o **PO9 Evaluación de riesgos**

- PO9.1 Marco de Trabajo de Administración de Riesgos
- PO9.2 Establecimiento del Contexto del Riesgo
- PO9.3 Identificación de Eventos
- PO9.4 Evaluación de Riesgos de TI
- PO9.5 Respuesta a los Riesgos
- PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos

Objetivo: Asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI

Para ello se logra la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos y se toma en consideración:

- Identificación, definición y actualización regular de los diferentes tipos de riesgos de TI (por ej.: tecnológicos, de seguridad, etc.) de manera de que se pueda determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable.
- Definición de alcances, limites de los riesgos y la metodología para las evaluaciones de los riesgos.
- Actualización de evaluación de riesgos

- Metodología de evaluación de riesgos
- Medición de riesgos cualitativos y/o cuantitativos
- Definición de un plan de acción contra los riesgos para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continúa.
- Aceptación de riesgos dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de que tan económico resulte implementar protecciones y controles.

o **PO10 Administración de proyectos**

- PO10.1 Marco de Trabajo para la Administración de Programas
- PO10.2 Marco de Trabajo para la Administración de Proyectos
- PO10.3 Enfoque de Administración de Proyectos
- PO10.4 Compromiso de los Interesados
- PO10.5 Declaración de Alcance del Proyecto
- PO10.6 Inicio de las Fases del Proyecto
- PO10.7 Plan Integrado del Proyecto
- PO10.8 Recursos del Proyecto
- PO10.9 Administración de Riesgos del Proyecto
- PO10.10 Plan de Calidad del Proyecto
- PO10.11 Control de Cambios del Proyecto
- PO10.12 Planeación del Proyecto y Métodos de Aseguramiento
- PO10.13 Medición del Desempeño, Reporte y Monitoreo del Proyecto
- PO10.14 Cierre del Proyecto

Objetivo: Establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión

Para ello se realiza una identificación y priorización de los proyectos en línea con el plan operacional por parte de la misma organización. Además, la organización deberá adoptar y aplicar sólidas técnicas de administración de proyectos para cada proyecto emprendido y se toma en consideración:

- Definición de un marco de referencia general para la administración de proyectos que defina el alcance y los límites del mismo, así como la metodología de administración de proyectos a ser adoptada y aplicada para cada proyecto emprendido. La metodología deberá cubrir, como mínimo, la asignación de responsabilidades, la determinación de tareas, la realización de presupuestos de tiempo y recursos, los avances, los puntos de revisión y las aprobaciones.

- El involucramiento de los usuarios en el desarrollo, implementación o modificación de los proyectos.

- Asignación de responsabilidades y autoridades a los miembros del personal asignados al proyecto.

- Aprobación de fases de proyecto por parte de los usuarios antes de pasar a la siguiente fase.

- Presupuestos de costos y horas hombre

- Planes y metodologías de aseguramiento de calidad que sean revisados y acordados por las partes interesadas.

- Plan de administración de riesgos para eliminar o minimizar los riesgos.

- Planes de prueba, entrenamiento, revisión post-implementación.

o **PO11 Administración de calidad**

- PO8.1 Sistema de Administración de Calidad

- PO8.2 Estándares y Prácticas de Calidad

- PO8.3 Estándares de Desarrollo y de Adquisición

- PO8.4 Enfoque en el Cliente de TI

- PO8.5 Mejora Continua

- PO8.6 Medición, Monitoreo y Revisión de la Calidad

Objetivo: Satisfacer los requerimientos del cliente

Para ello se realiza una planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización y se toma en consideración:

- Definición y mantenimiento regular del plan de calidad, el cual deberá promover la filosofía de mejora continua y contestar a las preguntas básicas de qué, quién y cómo.

- Responsabilidades de aseguramiento de calidad que determine los tipos de actividades de aseguramiento de calidad tales como revisiones, auditorias, inspecciones, etc. que deben realizarse para alcanzar los objetivos del plan general de calidad.

- Metodologías del ciclo de vida de desarrollo de sistemas que rija el proceso de desarrollo, adquisición, implementación y mantenimiento de sistemas de información.

- Documentación de pruebas de sistemas y programas

- Revisiones y reportes de aseguramiento de calidad

- **Dominio: Adquisición e implementación.** Para llevar a cabo la estrategia de TI, las soluciones de Ti deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

  ✓ **Procesos:**

  o **AI1 Identificación de Soluciones Automatizadas**

  - AI1.1 Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio

  - AI1.2 Reporte de Análisis de Riesgos

  - AI1.3 Estudio de Factibilidad y Formulación de Cursos de Acción Alternativos
  - AI1.4 Requerimientos, Decisión de Factibilidad y Aprobación

  Objetivo: Asegurar el mejor enfoque para cumplir con los requerimientos del usuario

Para ello se realiza un análisis claro de las oportunidades alternativas comparadas contra los requerimientos de los usuarios y toma en consideración:

- Definición de requerimientos de información para poder aprobar un proyecto de desarrollo.
- Estudios de factibilidad con la finalidad de satisfacer los requerimientos del negocio establecidos para el desarrollo de un proyecto.
- Arquitectura de información para tener en consideración el modelo de datos al definir soluciones y analizar la factibilidad de las mismas.
- Seguridad con relación de costo-beneficio favorable para controlar que los costos no excedan los beneficios.
- Pistas de auditoría para ello deben existir mecanismos adecuados. Dichos mecanismos deben proporcionar la capacidad de proteger datos sensitivos (ej. Identificación de usuarios contra divulgación o mal uso)
- Contratación de terceros con el objeto de adquirir productos con buena calidad y excelente estado.
- Aceptación de instalaciones y tecnología a través del contrato con el Proveedor donde se acuerda un plan de aceptación para las instalaciones y tecnología especifica a ser proporcionada.

o **AI2 Adquisición y mantenimiento del software aplicativo**

- AI2.1 Diseño de Alto Nivel
- AI2.2 Diseño Detallado
- AI2.3 Control y Posibilidad de Auditar las Aplicaciones
- AI2.4 Seguridad y Disponibilidad de las Aplicaciones
- AI2.5 Configuración e Implantación de Software Aplicativo Adquirido
- AI2.6 Actualizaciones Importantes en Sistemas Existentes
- AI2.7 Desarrollo de Software Aplicativo
- AI2.8 Aseguramiento de la Calidad del Software
- AI2.9 Administración de los Requerimientos de Aplicaciones

- AI2.10 Mantenimiento de Software Aplicativo

Objetivo: Proporciona funciones automatizadas que soporten efectivamente al negocio.

Para ello se definen declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros y se toma en consideración:

- Requerimientos de usuarios, para realizar un correcto análisis y obtener un software claro y fácil de usar.
- Requerimientos de archivo, entrada, proceso y salida.
- Interface usuario-maquina asegurando que el software sea fácil de utilizar y que sea capaz de auto documentarse.
- Personalización de paquetes
- Realizar pruebas funcionales (unitarias, de aplicación, de integración y de carga y estrés), de acuerdo con el plan de prueba del proyecto y con los estándares establecidos antes de ser aprobado por los usuarios.
- Controles de aplicación y requerimientos funcionales
- Documentación (materiales de consulta y soporte para usuarios) con el objeto de que los usuarios puedan aprender a utilizar el sistema o puedan sacarse todas aquellas inquietudes que se les puedan presentar.

o **AI3 Adquisición y mantenimiento de la infraestructura tecnológica**

- AI3.1 Plan de Adquisición de Infraestructura Tecnológica
- AI3.2 Protección y Disponibilidad del Recurso de Infraestructura
- AI3.3 Mantenimiento de la Infraestructura
- AI3.4 Ambiente de Prueba de Factibilidad

Objetivo: Proporcionar las plataformas apropiadas para soportar aplicaciones de negocios

Para ello se realizara una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la

instalación, seguridad y control del software del sistema y toma en consideración:

- Evaluación de tecnología para identificar el impacto del nuevo hardware o software sobre el rendimiento del sistema general.

- Mantenimiento preventivo del hardware con el objeto de reducir la frecuencia y el impacto de fallas de rendimiento.

- Seguridad del software de sistema, instalación y mantenimiento para no arriesgar la seguridad de los datos y programas ya almacenados en el mismo.

- **AI4 Desarrollo y mantenimiento de procedimientos**

  Objetivo: Asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas.

  Para ello se realiza un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento y toma en consideración:

  - Manuales de procedimientos de usuarios y controles, de manera que los mismos permanezcan en permanente actualización para el mejor desempeño y control de los usuarios.

  - Manuales de Operaciones y controles, de manera que estén en permanente actualización.

  - Materiales de entrenamiento enfocados al uso del sistema en la práctica diaria.

- **AI5 Instalación y aceptación de los sistemas**

  - AI7.1 Entrenamiento

  - AI7.2 Plan de Prueba

  - AI7.3 Plan de Implantación

  - AI7.4 Ambiente de Prueba

  - AI7.5 Conversión de Sistemas y Datos

  - AI7.6 Pruebas de Cambios

- AI7.7 Prueba de Aceptación Final.
- AI7.8 Promoción a Producción
- AI7.9 Revisión Posterior a la Implantación

Objetivo: Verificar y confirmar que la solución sea adecuada para el propósito deseado

Para ello se realiza una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas y toma en consideración:

- Capacitación del personal de acuerdo al plan de entrenamiento definido y los materiales relacionados.
- Conversión / carga de datos, de manera que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo.
- Pruebas específicas (cambios, desempeño, aceptación final, operacional) con el objeto de obtener un producto satisfactorio.
- Acreditación de manera que la Gerencia de operaciones y usuaria acepten los resultados de las pruebas y el nivel de seguridad para los sistemas, junto con el riesgo residual existente.
- Revisiones post implementación con el objeto de reportar si el sistema proporciono los beneficios esperados de la manera mas económica.

o **AI6 Administración de los cambios**

- AI6.1 Estándares y Procedimientos para Cambios
- AI6.2 Evaluación de Impacto, Priorización y Autorización
- AI6.3 Cambios de Emergencia
- AI6.4 Seguimiento y Reporte del Estatus de Cambio
- AI6.5 Cierre y Documentación del Cambio

Objetivo: Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores.

Esto se hace posible a través de un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual y toma en consideración:

- Identificación de cambios tanto internos como por parte de proveedores
- Procedimientos de categorización, priorización y emergencia de solicitudes de cambios.
- Evaluación del impacto que provocaran los cambios.
- Autorización de cambios
- Manejo de liberación de manera que la liberación de software este regida por procedimientos formales asegurando aprobación, empaque, pruebas de regresión, entrega, etc.
- Distribución de software, estableciendo medidas de control especificas para asegurar la distribución de software correcto al lugar correcto, con integridad y de manera oportuna.

- **Dominio: Entregar y Dar Soporte.** En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

  ✓ **Procesos**

  o **DS1 Definición de niveles de servicio**

  - DS1.1 Marco de Trabajo de la Administración de los Niveles de Servicio
  - DS1.2 Definición de Servicios
  - DS1.3 Acuerdos de Niveles de Servicio
  - DS1.4 Acuerdos de Niveles de Operación
  - DS1.5 Monitoreo y Reporte del Cumplimento de los Niveles de Servicio

- DS1.6 Revisión de los Acuerdos de Niveles de Servicio y de los Contratos

Objetivo: Establecer una comprensión común del nivel de servicio requerido

Para ello se establecen convenios de niveles de servicio que formalicen los criterios de desempeño contra los cuales se medirá la cantidad y la calidad del servicio y se toma en consideración:

- Convenios formales que determinen la disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de contingencia / recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio.

- Definición de las responsabilidades de los usuarios y de la función de servicios de información

- Procedimientos de desempeño que aseguren que la manera y las responsabilidades sobre las relaciones que rigen el desempeño entre todas las partes involucradas sean establecidas, coordinadas, mantenidas y comunicadas a todos los departamentos afectados.

- Definición de dependencias asignando un Gerente de nivel de Servicio que sea responsable de monitorear y reportar los alcances de los criterios de desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento.

- Provisiones para elementos sujetos a cargos en los acuerdos de niveles de servicio para hacer posibles comparaciones y decisiones de niveles de servicios contra su costo.

- Garantías de integridad

- Convenios de confidencialidad

- Implementación de un programa de mejoramiento del servicio.

o **DS2 Administración de servicios prestados por terceros**

- DS2.1 Identificación de Todas las Relaciones con Proveedores

- DS2.2 Gestión de Relaciones con Proveedores
- DS2.3 Administración de Riesgos del Proveedor
- DS2.4 Monitoreo del Desempeño del Proveedor

Objetivo: Asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos

Para ello se establecen medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes, en cuanto a su efectividad y suficiencia, con respecto a las políticas de la organización y toma en consideración:

- Acuerdos de servicios con terceras partes a través de contratos entre la organización y el proveedor de la administración de instalaciones este basado en niveles de procesamiento requeridos, seguridad, monitoreo y requerimientos de contingencia, así como en otras estipulaciones según sea apropiado.
- Acuerdos de confidencialidad. Además, se deberá calificar a los terceros y el contrato deberá definirse y acordarse para cada relación de servicio con un proveedor.
- Requerimientos legales regulatorios de manera de asegurar que estos concuerde con los acuerdos de seguridad identificados, declarados y acordados.
- Monitoreo de la entrega de servicio con el fin de asegurar el cumplimiento de los acuerdos del contrato.

o **DS3 Administración de desempeño y capacidad**

- DS3.1 Planeación del Desempeño y la Capacidad
- DS3.2 Capacidad y Desempeño Actual
- DS3.3 Capacidad y Desempeño Futuros
- DS3.4 Disponibilidad de Recursos de TI
- DS3.5 Monitoreo y Reporte

Objetivo: Asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado.
Para ello se realizan controles de manejo de capacidad y desempeño que recopilen datos y reporten acerca del manejo de cargas de trabajo, tamaño de aplicaciones, manejo y demanda de recursos y toma en consideración:

- Requerimientos de disponibilidad y desempeño de los servicios de sistemas de información
- Monitoreo y reporte de los recursos de tecnología de información
- Utilizar herramientas de modelado apropiadas para producir un modelo del sistema actual para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de configuración, desempeño y disponibilidad.
- Administración de capacidad estableciendo un proceso de planeación para la revisión del desempeño y capacidad de hardware con el fin de asegurar que siempre exista una capacidad justificable económicamente para procesar cargas de trabajo con cantidad y calidad de desempeño
- Prevenir que se pierda la disponibilidad de recursos mediante la implementación de mecanismos de tolerancia de fallas, de asignación equitativos de recursos y de prioridad de tareas.

o **DS4 Asegurar el Servicio Continuo**

- DS4.1 Marco de Trabajo de Continuidad de TI
- DS4.2 Planes de Continuidad de TI
- DS4.3 Recursos Críticos de TI
- DS4.4 Mantenimiento del Plan de Continuidad de TI
- DS4.5 Pruebas del Plan de Continuidad de TI
- DS4.6 Entrenamiento del Plan de Continuidad de TI
- DS4.7 Distribución del Plan de Continuidad de TI
- DS4.8 Recuperación y Reanudación de los Servicios de TI
- DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones

- DS4.10 Revisión Post Reanudación

Objetivo: mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones

Para ello se tiene un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio y toma en consideración:

- Planificación de Severidad
- Plan Documentado
- Procedimientos Alternativos
- Respaldo y Recuperación
- Pruebas y entrenamiento sistemático y singulares

o **DS5 Garantizar la seguridad de sistemas**

- DS5.1 Administración de la Seguridad de TI
- DS5.2 Plan de Seguridad de TI
- DS5.3 Administración de Identidad
- DS5.4 Administración de Cuentas del Usuario
- DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad
- DS5.6 Definición de Incidente de Seguridad
- DS5.7 Protección de la Tecnología de Seguridad
- DS5.8 Administración de Llaves Criptográficas
- DS5.9 Prevención, Detección y Corrección de Software Malicioso
- DS5.10 Seguridad de la Red
- DS5.11 Intercambio de Datos Sensitivos

Objetivo: salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida

Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración:

- Autorización, autenticación y el acceso lógico junto con el uso de los recursos de TI deberá restringirse a través de la instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso

- Perfiles e identificación de usuarios estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario

- Administración de llaves criptográficas definiendo implementando procedimientos y protocolos a ser utilizados en la generación, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas

- Manejo, reporte y seguimiento de incidentes implementado capacidad para la atención de los mismos

- Prevención y detección de virus tales como Caballos de Troya, estableciendo adecuadas medidas de control preventivas, detectivas y correctivas.

- Utilización de Firewalls si existe una conexión con Internet u otras redes públicas en la organización

o **DS6 Educación y entrenamiento de usuarios**

- DS6.1 Identificación de Necesidades de Entrenamiento y Educación

- DS6.2 Impartición de Entrenamiento y Educación

- DS6.3 Evaluación del Entrenamiento Recibido

Objetivo: Asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados.

Para ello se realiza un plan completo de entrenamiento y desarrollo y se toma en consideración:

- Currículo de entrenamiento estableciendo y manteniendo procedimientos para identificar y documentar las necesidades de entrenamiento de todo el personal que haga uso de los servicios de información

- Campañas de concientización, definiendo los grupos objetivos, identificar y asignar entrenadores y organizar oportunamente las sesiones de entrenamiento

- Técnicas de concientización proporcionando un programa de educación y entrenamiento que incluya conducta ética de la función de servicios de información

o **DS7 Identificación y asignación de costos**

- DS7.1 Definición de Servicios

- DS7.2 Contabilización de TI

- DS7.3 Modelación de Costos y Cargos

- DS7.4 Mantenimiento del Modelo de Costos

Objetivo: Asegurar un conocimiento correcto de los costos atribuibles a los servicios de TI

Para ello se realiza un sistema de contabilidad de costos que asegure que éstos sean registrados, calculados y asignados a los niveles de detalle requeridos y toma en consideración:

- Los elementos sujetos a cargo deben ser recursos identificables, medibles y predecibles para los usuarios

- Procedimientos y políticas de cargo que fomenten el uso apropiado de los recursos de computo y aseguren el trato justo de los departamentos usuarios y sus necesidades

- Tarifas definiendo e implementando procedimientos de costeo de prestar servicios, para ser analizados, monitoreados, evaluados asegurando al mismo tiempo la economía

o **DS8 Apoyo y asistencia a los clientes de TI**

Objetivo: asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente

Para ello se realiza un Buró de ayuda que proporcione soporte y asesoría de primera línea y toma en consideración:

- Consultas de usuarios y respuesta a problemas estableciendo un soporte de una función de buró de ayuda

- Monitoreo de consultas y despacho estableciendo procedimientos que aseguren que las preguntas de los clientes que pueden ser resueltas sean reasignadas al nivel adecuado para atenderlas

- Análisis y reporte de tendencias adecuado de las preguntas de los clientes y su solución, de los tiempos de respuesta y la identificación de tendencias

o **DS9 Administración de la configuración**

- DS9.1 Repositorio y Línea Base de Configuración

- DS9.2 Identificación y Mantenimiento de Elementos de Configuración

- DS9.3 Revisión de Integridad de la Configuración

Objetivo: Dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios

Para ello se realizan controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia y toma en consideración:

- Registro de activos estableciendo procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario, al momento de adquisición

- Administración de cambios en la configuración asegurando que los registros de configuración reflejen el status real de todos los elementos de la configuración

- Chequeo de software no autorizado revisando periódicamente las computadoras personales de la organización

- Controles de almacenamiento de software definiendo un área de almacenamiento de archivos para todos los elementos de software válidos en las fases del ciclo de vida de desarrollo de sistemas

- **DS10 Administración de Problemas**

  - DS10.1 Identificación y Clasificación de Problemas
  - DS10.2 Rastreo y Resolución de Problemas
  - DS10.3 Cierre de Problemas
  - DS10.4 Integración de las Administraciones de Cambios, Configuración y Problemas

  Objetivo: Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder.

  Para ello se necesita un sistema de manejo de problemas que registre y dé seguimiento a todos los incidentes, además de un conjunto de procedimientos de escalamiento de problemas para resolver de la manera más eficiente los problemas identificados. Este sistema de administración de problemas deberá también realizar un seguimiento de las causas a partir de un incidente dado.

- **DS11 Administración de Datos**

  - DS11.1 Requerimientos del Negocio para Administración de Datos
  - DS11.2 Acuerdos de Almacenamiento y Conservación
  - DS11.3 Sistema de Administración de Librerías de Medios
  - DS11.4 Eliminación
  - DS11.5 Respaldo y Restauración
  - DS11.6 Requerimientos de Seguridad para la Administración de Datos

  Objetivo: Asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento.

  Lo cual se logra a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI. Para tal fin, la gerencia deberá diseñar formatos de entrada de datos para los usuarios de manera que se minimicen lo errores y las omisiones durante la creación de los datos.

Este proceso deberá controlar los documentos fuentes (de donde se extraen los datos), de manera que estén completos, sean precisos y se registren apropiadamente. Se deberán crear también procedimientos que validen los datos de entrada y corrijan o detecten los datos erróneos, como así también procedimientos de validación para transacciones erróneas, de manera que éstas no sean procesadas. Cabe destacar la importancia de crear procedimientos para el almacenamiento, respaldo y recuperación de datos, teniendo un registro físico (discos, disquetes, CDs y cintas magnéticas) de todas las transacciones y datos manejados por la organización, albergados tanto dentro como fuera de la empresa.

La gerencia deberá asegurar también la integridad, autenticidad y confidencialidad de los datos almacenados, definiendo e implementando procedimientos para tal fin.

- **DS12 Administración de las instalaciones**

  - DS12.1 Selección y Diseño del Centro de Datos
  - DS12.2 Medidas de Seguridad Física
  - DS12.3 Acceso Físico
  - DS12.4 Protección Contra Factores Ambientales
  - DS12.5 Administración de Instalaciones Físicas

  Objetivo: Proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

- **DS13 Administración de la operación**

  - DS13.1 Procedimientos e Instrucciones de Operación
  - DS13.2 Programación de Tareas
  - DS13.3 Monitoreo de la Infraestructura de TI
  - DS13.4 Documentos Sensitivos y Dispositivos de Salida

- DS13.5 Mantenimiento Preventivo del Hardware

Objetivo: Asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada.

Esto se logra a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Para ello, la gerencia deberá establecer y documentar procedimientos para las operaciones de tecnología de información (incluyendo operaciones de red), los cuales deberán ser revisados periódicamente para garantizar su eficiencia y cumplimiento.

- **Dominio: Monitoreo.** Todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad. Este es, precisamente, el ámbito de este dominio.

  ✓ **Procesos**

  o **M1 Monitoreo del Proceso**

  - ME1.1 Enfoque del Monitoreo
  - ME1.2 Definición y Recolección de Datos de Monitoreo
  - ME1.3 Método de Monitoreo
  - ME1.4 Evaluación del Desempeño
  - ME1.5 Reportes al Consejo Directivo y a Ejecutivos
  - ME1.6 Acciones Correctivas

  Objetivo: Asegurar el logro de los objetivos establecidos para los procesos de TI. Lo cual se logra definiendo por parte de la gerencia reportes e indicadores de desempeño gerenciales y la implementación de sistemas de soporte así como la atención regular a los reportes emitidos.

  Para ello la gerencia podrá definir indicadores claves de desempeño y/o factores críticos de éxito y compararlos con los niveles objetivos propuestos para evaluar el desempeño de los procesos de la organización. La gerencia deberá también medir el grado de satisfacción del los clientes con respecto a los servicios de información proporcionados para identificar deficiencias en los niveles de servicio y establecer

objetivos de mejoramiento, confeccionando informes que indiquen el avance de la organización hacia los objetivos propuestos.

- **M2 Evaluar lo adecuado del Control Interno**

  - ME2.1 Monitoreo del Marco de Trabajo de Control Interno
  - ME2.2 Revisiones de Auditoría
  - ME2.3 Excepciones de Control
  - ME2.4 Auto Evaluación del Control
  - ME2.5 Aseguramiento del Control Interno
  - ME2.6 Control Interno para Terceros
  - ME2.7 Acciones Correctivas

  Objetivo: Asegurar el logro de los objetivos de control interno establecidos para los procesos de TI.

  Para ello la gerencia es la encargada de monitorear la efectividad de los controles internos a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias., evaluar su efectividad y emitir reportes sobre ellos en forma regular. Estas actividades de monitoreo continuo por parte de la Gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

- **M3 Obtención de Aseguramiento Independiente**

  - ME3.1 Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales
  - ME3.2 Optimizar la Respuesta a Requerimientos Externos
  - ME3.3 Evaluación del Cumplimiento con Requerimientos Externos
  - ME3.4 Aseguramiento Positivo del Cumplimiento
  - ME3.5 Reportes Integrados

  Objetivo: Incrementar los niveles de confianza entre la organización, clientes y proveedores externos. Este proceso se lleva a cabo a intervalos regulares de tiempo.

Para ello la gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de tecnología de información que resulten críticos, como así también para trabajar con nuevos proveedores de servicios de tecnología de información. Luego la gerencia deberá adoptar como trabajo rutinario tanto hacer evaluaciones periódicas sobre la efectividad de los servicios de tecnología de información y de los proveedores de estos servicios como así también asegurarse el cumplimiento de los compromisos contractuales de los servicios de tecnología de información y de los proveedores de estos servicios.

- **M4 Proveer Auditoria Independiente**

  - ME4.1 Establecimiento de un Marco de Gobierno de TI
  - ME4.2 Alineamiento Estratégico
  - ME4.3 Entrega de Valor
  - ME4.4 Administración de Recursos
  - ME4.5 Administración de Riesgos
  - ME4.6 Medición del Desempeño
  - ME4.7 Aseguramiento Independiente

  Objetivo: Incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de auditorías independientes desarrolladas a intervalos regulares de tiempo. Para ello la gerencia deberá establecer los estatutos para la función de auditoría, destacando en este documento la responsabilidad, autoridad y obligaciones de la auditoria. El auditor deberá ser independiente del auditado, esto significa que los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado y en lo posible deberá ser independiente de la propia empresa.

Esta auditoría deberá respetar la ética y los estándares profesionales, seleccionando para ello auditores que sean técnicamente competentes, es decir que cuenten con habilidades y conocimientos que aseguren tareas efectivas y eficientes de auditoría.

La función de auditoría deberá proporcionar un reporte que muestre los objetivos de la auditoria, período de cobertura, naturaleza y trabajo de auditoría realizado,

como así también la organización, conclusión y recomendaciones relacionadas con el trabajo de auditoría llevado a cabo.

Los 34 procesos propuestos se concretan en 32 objetivos de control detallados anteriormente.

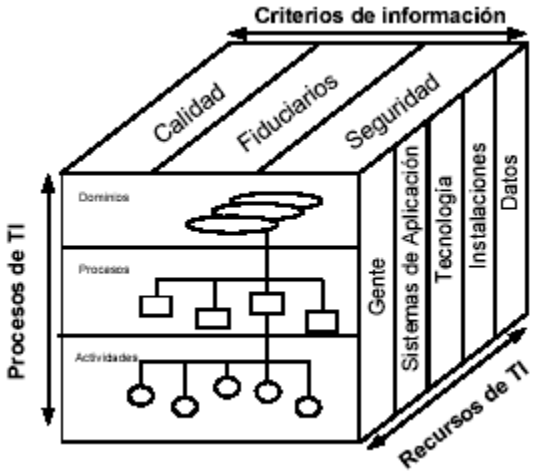
Un Control se define como "las normas, estándares, procedimientos, usos y costumbres y las estructuras organizativas, diseñadas para proporcionar garantía razonable de que los objetivos empresariales se alcanzaran y que los eventos no deseados se preverán o se detectaran, y corregirán"

Un Objetivo de Control se define como "la declaración del resultado deseado o propuesto que se ha de alcanzar mediante la aplicación de procedimientos de control en cualquier actividad de TI".

En resumen, la estructura conceptual se puede enfocar desde tres puntos de vista:

- Los recursos de las TI
- Los criterios empresariales que deben satisfacer la información
- Los procesos de TI

Figura 1: Las tres dimensiones conceptuales de COBIT



Las tres dimensiones conceptuales de COBIT
COBIT 4.1

Estos dominios facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

Además, se toma en cuenta los recursos que proporciona la tecnología de información, tales como: datos, aplicaciones, plataformas tecnológicas, instalaciones y recurso humano.

Toda organización, necesita desarrollar una tecnología que le permita rediseñar actividades y procesos para lograr un mejor desempeño en las mismas, es así como el COBIT es fundamental en toda empresa, pues esta metodología reduce posibles vulnerabilidades y riesgos de los recursos de las tecnologías de información y así mismo evalúa el resultado de los objetivos de la empresa.

1.6.2. COSO (Sponsoring Organizations of the Treadway Commission). COSO inicio en 1985 recomendando que las organizaciones patrocinadoras de la Comisión trabajen juntas para desarrollar sistemas integrados de orientación sobre el control interno.

El modelo COSO define el control interno como un conjunto de procesos, realizado por los directivos de una organización, y creado para garantizar el logro de los objetivos.

COSO consta de cinco elementos, estos elementos proporcionan un marco eficaz para describir y analizar el sistema de control interno, los cuales son:

- **Entorno de control.** Sirve como base para los demás componentes del control interno, proporcionando disciplina y estructura. Los factores del entorno de control incluyen la integridad, los valores éticos, el estilo de funcionamiento de la administración, la delegación de los sistemas de autoridad, así como los procesos de gestión y desarrollo de las personas en la empresa.

- **Evaluación del riesgo.** Cada empresa se enfrenta a una variedad de riesgos de fuentes externas e internas que deben ser evaluados. Una condición previa para la evaluación de riesgos es el establecimiento de objetivos y por lo tanto la evaluación de riesgos es la caracterización y análisis de los riesgos relevantes para la consecución de los objetivos asignados. La evaluación de riesgos es un requisito previo para establecer cómo los riesgos deberían ser manejados.

- **Las actividades de control.** Las actividades de control son las políticas y procedimientos que ayudan a asegurar la gestión de las directivas se llevan a cabo. También garantizan la toma de medidas necesarias para hacer frente a los riesgos que pueden obstaculizar el logro de los objetivos de la entidad. Las actividades de control se originan en toda la organización, en todos los niveles y en todas las funciones. Estos incluyen una amplia gama de actividades tan diversas como aprobaciones, autorizaciones, verificaciones, conciliaciones,

revisiones de desempeño operativo, la seguridad de los activos y la separación de funciones.

- **Información y comunicación.** Los sistemas de información juegan un papel importante en los sistemas de control interno que producen los informes, incluidos los operativos, financieros y el cumplimiento de información relacionada, que permiten elaborar y controlar la entidad. De manera más amplia, la comunicación eficaz debe garantizar los flujos de información hacia abajo, y hasta a través de la organización.

- **Seguimiento.** Los sistemas de control interno deben ser supervisados, un proceso que evalúa la calidad del desempeño del sistema en el tiempo. Esto se logra a través de continuas actividades de supervisión o evaluaciones por separado. Las fallas de control interno detectadas a través de estas actividades deberían notificar las medidas de planificación y correctivas garantizando la mejora continua del sistema.

  Algunas diferencias entre COSO y COBIT, que son los dos modelos más difundidos actualmente son:

  - ✓ El modelo COSO está enfocado a toda la empresa, mientras que el COBIT se limita a las tecnologías de la información (TI).

  - ✓ El COBIT establece como uno de sus objetivos la seguridad de la información, por el contrario COSO, no lo toma en cuenta en su evaluación.

El modelo de control interno que presenta el COSO no es muy completo, a diferencia de la metodología COBIT que contempla políticas, procedimientos y estructuras organizativas, además de procesos para definir el modelo de control interno.

1.7. TÉCNICAS DE AUDITORIA DE SISTEMAS

1.7.1. Selección de áreas de auditoria. Dada la magnitud del universo por auditar, la revisión debe hacerse de manera selectiva, esta técnica es adecuada para empresas con múltiples localizaciones o sucursales, con el fin de dar prioridad a los procesos, se aplican evaluaciones estadísticas a estos en forma periódica, para poder clasificar cuales de estos procesos son claves para el proceso de auditoría.

El uso del computador es indispensable en esta técnica ya que se manejan grandes volúmenes de información y los tamaños de muestra son muy grandes,

además esta herramienta mejora la efectividad y eficiencia de los procesos de auditoría, también proporciona pruebas de control efectivas.

Una desventaja de esta técnica es que la construcción de estos modelos es costosa y consume demasiado tiempo y se deben tener conocimientos avanzados y especializados en materia de diseño y construcción.

- **Simulación – Modelaje.** Esta técnica consiste en la creación de modelos conceptuales o físicos bajo ciertas condiciones y simular el comportamiento del sistema computacional, de un programa, o evaluar el sistema financiero en forma periódica(evaluar el incremento o decremento de las cuentas contables o áreas financieras en términos de ingresos, egresos y gastos, para determinar el crecimiento organizacional), estos modelos brindan la posibilidad de realizar pruebas controladas o realizar comparaciones entre valores proyectados y valores reales en materia financiera, con los resultados obtenidos en la simulación el auditor puede dar una opinión acerca del rendimiento del sistema y también proponer medidas de contingencia al respecto.

- **Sistema de puntajes (Scoring).** A diferencia de las anteriores técnicas la evaluación a los procesos y aplicaciones computarizadas se realiza de forma manual, con el fin de priorizar procesos con base en el análisis de riesgos, con la asignación de valores numéricos a las características claves, el auditor asignara la ponderación que este considere para cada factor, teniendo en cuenta el análisis de riesgo realizado con anterioridad que permita obtener un alto grado de confiabilidad , para llevar a cabo esta técnica se deberá diligenciar un formato de puntajes el que dará por resultado la clasificación para la auditoria.

1.7.2. Técnicas para operacionalizar la función de auditoría

- **Software de auditoria multisitio.** Es una técnica aplicable a grandes empresas que tengan diferentes centros electrónicos de datos (PED, Procesamiento electrónico de datos). Desarrollando un programa o grupo de programas e instalándolos en las regionales para que sean utilizados por los auditores. Se requiere que se guarde uniformidad en el software utilizado en los PED para facilitar el proceso de auditaje, esta técnica es aplicada en ambientes de procesamiento distribuido.

- **Centros de competencia.** Esta técnica funciona a la inversa que la técnica de multisitio, ya que centra toda la información de las regionales en un centro de

competencia y después de su análisis, evaluación e informes son enviados a las sucursales para tomar las respectivas decisiones.

1.7.3. Técnicas para probar controles de sistemas en funcionamiento

- **Métodos de datos de prueba.** Las técnicas de datos de prueba se usan durante una auditoría alimentando datos en el sistema de computadora de una entidad y comparando los resultados obtenidos con resultados predeterminados. Un elemento de gran importancia en esta técnica es el diseño de los datos de prueba, lo que en últimas determinara la efectividad de esta técnica. Es recomendable seleccionar datos normales, ilógicos, imposibles, con valores extremos, etc. Un auditor podría usar esta técnica para:

  - ✓ Poner a prueba los controles específicos en los programas de cómputo, como son la clave de acceso en línea y los controles para el acceso a datos.

  - ✓ Colocar a prueba transacciones de prueba seleccionadas a partir de transacciones anteriores o creadas por el auditor para verificar las características específicas de procesamiento del sistema de cómputo de una dependencia. En general, estas transacciones se procesan fuera del procesamiento normal que utilice la dependencia.

  - ✓ Poner a prueba transacciones usadas en un mecanismo integrado de pruebas donde se establece una unidad modelo (por ejemplo, un departamento o empleado ficticio), a la cual se le registran las transacciones durante el ciclo de procesamiento normal.

  - ✓ Realizar pruebas de cumplimiento de los controles generales, por ejemplo, el uso de datos de prueba para verificar los procedimientos de acceso a las bibliotecas del programa.

  - ✓ Pruebas de cumplimiento de los controles de aplicación, por ejemplo, el uso de los datos de prueba para verificar el funcionamiento de un procedimiento programado.

  Cuando se procesan los datos de prueba con el procesamiento normal de la entidad, el auditor se asegura de que las transacciones de prueba sean eliminadas posteriormente de los registros contables de la entidad.

  Se debe tener en cuenta que si se trata de una entidad pequeña y se procesan volúmenes menores de datos, los métodos manuales pueden ser de costo más efectivo.

En los procedimientos de auditoría para controlar las aplicaciones de datos de prueba se deben realizar las siguientes acciones:

- ✓ Controlar la secuencia de presentación de datos de prueba cuando se extienda a varios ciclos de procesamiento.

- ✓ Realizar corridas de prueba que contengan pequeñas cantidades de datos de prueba antes de presentar los datos de prueba principales de la auditoría.

- ✓ Predecir los resultados de los datos de prueba y compararlos con la salida real de datos de pruebas, para las transacciones individuales.
- ✓ Confirmar que se usó la versión actual de los programas para procesar los datos de prueba.

- ✓ Poner a prueba si los programas usados para procesar los datos de prueba fueron utilizados por la entidad durante el periodo aplicable de auditoría.

En síntesis se puede emplear esta técnica para: evaluación de controles específicos, verificación de validaciones, prueba de perfiles de acceso, prueba a transacciones seleccionadas con las siguientes ventajas y desventajas:

- ✓ **Ventajas**

  - o Se empieza por el inicio, tratando de verificar que el aplicativo este en capacidad de validar cualquier tipo de dato introducido en el sistema dejando por supuesto que se ingresen los validos y advirtiendo del intento de ingreso de datos incorrectos.

  - o En la mayoría de los casos la información resultado estará protegida y libre de errores cuando el aplicativo permita validar los tipos de datos ingresados al sistema.

- ✓ **Desventajas**

  - o Para obtener resultados preestablecidos posiblemente no se los pueda obtener de forma manual puesto que algunos procedimientos de auditoría dependen de un procesamiento mucho más complejo que otros (por ejemplo, análisis estadístico avanzado) o implica cantidades de datos que sobrepasarían cualquier procedimiento manual, implicaría la creación de módulos secuenciales de prueba para obtener dichos resultados.

  - o Al utilizarlas en sistemas que están en la etapa de producción genera costos por los retazos ocasionados al hacer las respectivas pruebas.

- **Evaluación del sistema en caso base (BCSE).** Cuando la técnica de datos de prueba se mantiene en el tiempo para ser, consistente y cotidianamente, aplicada al sistema en producción, toma el nombre de EVALUACION DEL SISTEMA DEL CASO BASE (ESCB), en tal caso, la prueba es más completa y requiere de un alto grado de cooperación entres usuarios, auditores y personal de sistemas.

  Esta técnica se utiliza en auditorias que hacen uso de controles preventivos y detectivos a los sistemas, los cuales manejan aplicativos para sistemas contables, sistema de nomina, sistemas estadísticos, etc., y en fin sistemas que deban validar los campos de datos que se ingresarán al aplicativo, y de forma paralela evaluar los procedimientos internos del sistema.

  ✓ **Ventajas**

  - Alta seguridad en los resultados que se van a obtener, puesto que para crear los datos de prueba se hacen participes los auditores, usuarios y el personal de sistemas que prepararán un material mucho más eficiente para ser objeto de la auditoria.

  - Al no abandonarse la prueba en el sistema caso base se puede perfeccionar el sistema ya que cuando se deje de encontrar errores adicionales de lógica o procesamiento se podría decir que se ha creado una versión mejorada de dicha aplicación, para poder desarrollar de mejor manera los cálculos a los datos introducidos a la aplicación y retornar información más confiable.

  ✓ **Desventajas**

  - Se necesitará preparar resultados pre calculados de forma manual para compararlos con los arrojados por el aplicativo.

  - El uso de mayor tiempo y de personal.

- **Operación Paralela.** También conocida como pruebas de cumplimiento, se realiza una copia del sistema.

  Su uso radica en auditorias donde se haga uso de controles correctivos a los sistemas de información que cuentan con un mecanismo de procesamiento en donde de antemano se sabe que posee algún tipo de error ya sea en su lógica de procesamiento al momento de realizar transacciones o en cálculos matemáticos.

✓ **Ventajas**

- El hecho de llevar de la mano el sistema actual con el nuevo se convierte en una ventaja ya que se va a garantizar que el sistema nuevo funcione de la mejor manera posible, a fin de evitar futuras modificaciones en su lógica o procesamiento.

- Convertir un sistema ya sea manual o computarizado el cual presente algunas falencias, en un sistema mucho más eficiente y con mayor probabilidad de generar cálculos e información mucho más veraz y rápida.

✓ **Desventajas**

- Si el sistema actual falla por lógica de procedimiento o por cálculos, el sistema nuevo también va ha fallar puesto que van de la mano.

- **Facilidad de prueba integrada (Integrated Test Facility).** Su objetivo y uso es similar método de datos de prueba pero su gran diferencia principal radica en que su implementación se realiza sin detener el funcionamiento normal de la instalación, mezclando los datos de prueba con los datos reales, en la misma aplicación.

  En esta técnica se realiza un procesamiento simultáneo de datos de prueba que representan operaciones ficticias en un conjunto con datos de operaciones reales, durante un procesamiento real. Esto permite al auditor comparar los resultados de procesamiento de datos de prueba con los resultados previamente determinados. Si los resultados del procesamiento de los datos de prueba resultan conforme a lo esperado, es razonable suponer que el programa de computación procesa los datos reales tal como corresponde.

  Esta técnica no se propone revisar la validez de los datos de entrada sino que prueba la validez de los programas de computación que procesan los datos de entrada, a efectos de determinar si operan de conformidad con su diseño previamente aprobado.

  Esta técnica se utiliza en auditorias donde exista disposición de los datos reales de la entidad. Es optima cuando se utilizan para auditar los controles defectivos en los sistemas, se utiliza en auditorías externas de sistemas que manejen gran cantidad de tipos de datos en una única transacción, como son sistemas contables, sistema de nomina, sistemas estadísticos, etc., puesto que sus resultados arrojaran un informe intachable.

✓ **Ventajas**

- No requiere una considerable pericia técnica por parte del auditor, sino más bien conocimiento y comprensión sobre el sistema.
- Se utilizan datos reales y por ende se auditará cualquier tipo de transacción de las posibles que soporte el sistema.
- No es necesario solicitar la colaboración del equipo, puesto que las transacciones de prueba se procesan simultáneamente con las reales de la entidad.
- Los resultados e informes obtenidos a través de la entidad ficticia permitirán de forma segura e inmediata analizar la eficiencia del sistema auditado.

✓ **Desventajas**

- Existe la posibilidad de afectar la integridad de la información real.
- Se requiere de un método efectivo que permita eliminar los informes producidos por la entidad ficticia, puesto que se podría borrar información real del sistema.

- **Simulación en paralelo.** Programas independientes creados por la auditoría para procesar datos reales y simular proceso real.

  Esta es una técnica en la que el auditor elabora, a través de lenguajes de programación o programas utilitarios avanzados, una aplicación similar a la que va a ser auditada, con el objetivo de ingresar simultáneamente la misma información en ambas aplicaciones para verificar la exactitud del procesamiento de datos de la aplicación en producción.

  También denominadas pruebas sustantivas, evaluación de la comparación entre los resultados de dos sistemas diferentes que han recibido los mismos datos de entrada. Simulación total o parcial de componentes del sistema.

  Esta técnica se utiliza en auditorias donde se tiene deposición de los datos reales de la entidad, por otra parte se utiliza para verificar controles detectivos en sistemas que manejan aplicativos software como son sistema contable, sistema de nomina, sistemas estadísticos, etc., con el fin de realizar control a la lógica de la aplicación y la precisión de los respectivos cálculos.

- ✓ **Ventajas**

  - o Posee mayor disponibilidad de información, puesto que lo que hace es trabajar con los datos reales con los que cuenta la entidad auditada para sus procesos internos. De esta forma no se quedara sin ser evaluada ningún tipo de transacción de las que realiza el aplicativo de forma normal.

  - o Al trabajar con datos reales se hace más confiables los informes resultado que se esperan obtener.

- ✓ **Desventajas**

  - o Se hace necesario preparar módulos computarizados que simulen la aplicación real para poder obtener los resultados con los cuales se comparará los resultados obtenidos en la aplicación real.

1.7.4. Técnicas para seleccionar y monitorear transacciones. Los procedimientos de auditoría son distintos de acuerdo con la filosofía y técnica de cada organización o entidad o de cada departamento. De ahí que se desprendan auditorias de todo tipo entre las que se encuentran las de informática que a su vez se dividen en categorías como las de métodos manuales y las de métodos asistidos por computadoras.

Por lo tanto cuando una auditoria se conduce en un entorno de CIS ("Auditoria en un entorno de sistemas de información por computadora") sus objetivos y su alcance no cambian a través del proceso, pero al aplicar los procedimientos de auditoría, se puede requerir técnicas que usen la computadora como una herramienta para dicha auditoria. A los usos diversos que se le pueden dar a la computadora se los conoce como Técnicas de Auditoria con Ayuda de Computadora (TAACs).

Estas técnicas son relativamente nuevas y son usadas generalmente por altas organizaciones que necesitan analizar información en grandes volúmenes, con las llamadas TAACs la auditoria se centra en el análisis de datos y no en la recolección de los mismos, además inmersas en las TAACs podremos encontrar modelos de auditoría como los siguientes:

- Selección de transacciones de entrada.

- Archivo de revisión de auditoría como control del sistema (SCARF).

- Archivo de revisión de auditoría por muestreo (SARF).

- Registros extendidos.

A partir de este análisis se pueden inferir algunos usos de las TAACs en general y cuando se las debe aplicar; un ejemplo claro es cuando la escases de documentos de entrada o la nula visibilidad del proceso de auditoría puede requerir el uso de las TAACs en la aplicación de procedimientos de cumplimiento, además estos procesos se pueden mejorar en eficiencia y efectividad mediante el uso de esas TAACs.

La necesidad de controlar el procesamiento electrónico de datos en cualquier entidad con el objetivo de garantizar el control permanente de las transacciones y de sus derivados hacen de las siguientes técnicas de auditoría, fundamentales en cualquier entidad, por lo tanto los escenarios de uso de estas técnicas de auditoría son innumerables en áreas que necesiten controlar anomalías que se susciten en sus procesos.

- **Selección de Transacciones de Entrada.** Esta técnica es ejecutada por un software de auditoría el cual es independiente a todos los sistemas, consiste en seleccionar y separar datos de entrada que son parte de las aplicaciones. Y se las hace en base al criterio del auditor.

  Entre las ventajas más significativas de este método es la seguridad del método ya que no cabe espacio para el fraude o el error, ya que el riesgo de alteración de los datos del sistema es evidentemente bajo.

  Se utiliza en auditorias para verificar los controles detectivos utilizados en sistemas de información computarizados que hayan sido modificados con el fin de verificar el buen funcionamiento de la lógica y los cálculos matemáticos.

  ✓ **Ventajas**

  - Esta técnica es relativamente fácil de aplicar.
  - No necesita modificar el código fuente de la aplicación.
  - No se presentan riesgos de alteración de la información generada por el sistema.

  ✓ **Desventajas**

  - Se requiere de un aplicativo que permita seleccionar los datos de entrada y las transacciones dependiendo de los parámetros que crea pertinente el auditor.

- **Archivo de Revisión de auditoría como control del sistema (SCARF).** Este tipo de técnica consiste en incorporar aplicaciones de auditoria dentro del sistema para que ejecute rutinas de supervisión y monitoreo en forma permanente. La aplicación de este tipo de software se conoce como subrutina, a partir de esta subrutina se seleccionaran muestreos previamente definidos.

  Esta técnica se utiliza en sistemas que manejan aplicativos software como son sistema contable, sistema de nomina, sistemas estadísticos, etc., los cuales manejan una gran numero de diversos tipos de transacciones con el fin de realizar control a la lógica de la aplicación y la precisión de los respectivos cálculos.

  ✓ **Ventajas**

  - Con esta técnica no solo se obtiene resultados para ser comparados sino que permite, supervisar, obtener muestreos y reportes de excepciones al momento de desarrollarse una transacción en el aplicativo.

  - Este tipo de técnica permiten auditar de forma más continua las transacciones producidas por un aplicativo, puesto que se incrustan módulos que permiten controlar de forma permanente el desarrollo de las transacciones.

  - Permite abrir una ventana en la caja negra, para observar y controlar el proceso de la transacción.

  ✓ **Desventajas**

  - Trabaja con un gran número de transacciones, dependiendo del peso de trabajo que tenga el aplicativo de la entidad.

  - Se hace necesario preparar e implantar las rutinas de auditoría a la medida para las aplicaciones software de la entidad auditada, lo que requiere tiempo y costos.

  - Se requiere pericia técnica por parte del auditor.

  - Necesidad de intervención activa del auditor durante las diversas etapas de su desarrollo y aplicación.

- **Archivo de revisión de auditoria por muestreo (SARF).** Esta técnica es muy parecida a SCARF, la diferencia radica en que la selección de las transacciones ya no se hacen en forma automática predefiniéndolas sino que por el contrario

se realizan al azar, esto con el fin de capturar archivos representativos para analizarlos con el apoyo de la estadística.

Se requiere un analista de sistema o programador para que preparen los módulos a decisión del auditor.

Esta técnica se utiliza para auditar sistemas que tengan gran carga de trabajo en cuanto a variedad de transacciones se refiere como son sistemas que manejan aplicativos contable en bancos, aerolíneas, etc.

- ✓ **Ventajas**

  - o Posibilita el monitoreo permanente de la ejecución de una transacción particular del sistema.

  - o Permite abrir una ventana en la caja negra, para observar y controlar el proceso de la transacción reduciendo la posibilidad de fraude de la información.

  - o No trabaja con un gran número de transacciones, puesto que las selecciona al azar ya que se apoya en muestreos estadísticos.

- ✓ **Desventajas**

  - o Se hace necesario preparar e implantar los módulos de auditoría a la medida para las aplicaciones software de la entidad auditada, lo que requiere tiempo y costos.

  - o Se requiere pericia técnica por parte del auditor.

  - o Necesidad de intervención activa del auditor durante las diversas etapas de su desarrollo y aplicación.

- **Registros Extendidos.** Con la aplicación de pequeñas rutinas se recogen datos que han afectado el funcionamiento del sistema, todo este tipo de rutina se conocen como pistas de auditoría, los cuales dejan un historial de todas las actividades secuencias y/o fallos del sistema.

  Esta técnica se utiliza en auditorias para verificar los controles detectivos y correctivos en sistemas que manejan aplicativos software como son sistema contable de bancos, sistema de nomina, sistemas estadísticos, etc. con el fin de obtener una pista de toda la información clave de las diferentes transacciones.

- ✓ **Ventajas**

  - o Se incluye en algún tipo de registro información significativa sobre las transacciones o el sistema, que luego pude ser consultada por el auditor.

  - o Al igual que en SCARF este tipo de registros permiten auditar de forma más continua las transacciones producidas por los aplicativos software.

  - o Al guardar en un solo registro cualquier tipo de modificación que se hagan a las transacciones, será más fácil encontrar la causa de que se produzca algún tipo de información errónea o no valida.

- ✓ **Desventajas**

  - o Se hace necesario preparar e implantar las rutinas de auditoría a la medida para las aplicaciones software de la entidad auditada, lo que requiere tiempo y costo de desarrollo.

  - o Se requiere pericia técnica por parte del auditor.

  - o Necesidad de intervención activa del auditor durante las diversas etapas de su desarrollo y aplicación.

1.7.5. Técnicas para la auditoria de información almacenada. El fin de un proceso auditor es asistir a la gerencia o al departamento auditado para brindar apoyo en la identificación de los diversos hallazgos y posibles riesgos, y formular soluciones que sirvan para el control que eviten estos errores y minimicen los riesgos, generalmente algunas tareas del proceso auditor toman demasiado tiempo como por ejemplo el planteamiento, desarrollo y documentación; la automatización de algunas tareas puede resultar muy productivo para el equipo auditor, especialmente en el caso de auditoría de sistemas donde algunos procesos se prestan para ser automatizados.

Estos procesos toman cada vez más fuerza a nivel mundial después de lo acontecido con los desfalcos que llevaron a la quiebra a grandes empresas como Parmalat (italiana) y Enron (norteamericana) los cual replantea el proceso de auditoría tanto interna, como externa y la utilización de herramientas informáticas tanto de nivel general como herramientas especializadas.

La automatización como se menciona anteriormente, se facilita para algunos procesos en la auditoria de sistemas, lo cual brinda algunos beneficios como la clara reducción en el tiempo y posiblemente de recursos en el desarrollo del proceso automatizado, la estandarización en los procesos y a su vez una mayor flexibilidad ante los cambios lo cual se puede ver reflejado en una mejora en la

calidad, provee mecanismos de monitoreo y retroalimentación, además la posibilidad de realizar análisis con diversos criterios, tales como recalculo de operaciones, búsqueda avanzada de información, seguimiento de transacciones, etc., convirtiéndose así en un poderoso aliado del equipo auditor permitiéndoles enfocarse en otros campos y obtener así un mejor y más profundo resultado.

El avance tecnológico que se ha vivido en los últimos años en el mundo ha generado la importancia para las personas y empresas de mantenerse actualizado e informado, pero esta información debe cumplir con ciertas características importantes como la veracidad, confiabilidad y oportunidad de la misma. Con el fin de obtener y gestionar esta información han surgido las NTIC (Nuevas Tecnologías de la Información y la comunicación); gracias a esto la información que se ha convertido en uno de los más valiosos recursos en las empresas, puede ser obtenida, tratada y almacenada para una mejor toma de decisiones.

Al introducir una herramienta tan poderosa como el computador en el proceso de auditoría esto conlleva a la utilización de herramientas informáticas para analizar la información que en su gran mayoría se encuentra en medios de almacenamiento magnético (discos duros, cd, dvd), con esto se busca evaluar la consistencia que presentan los sistemas de información, análisis de datos de una muestra de transacciones para verificar la integridad, consistencia y confiabilidad de la información presentada a través de los sistemas de información, el auditor debe desarrollar procedimientos en el que se consideren la herramientas informáticas como apoyo para la realización de la auditoria.

- **Aplicaciones estandarizadas para grandes volúmenes de información.** Es indispensable que las empresas realicen auditorias rigurosas frecuentemente, especialmente a las áreas más sensibles del negocio, realizar un manual del comportamiento de la empresa con las normas y procedimientos internos.

  ✓ **Ventajas**

  - Controlar el riesgo de fraudes en las empresas, para que se disminuyan las constantes quiebras empresariales que causaron fuertes impactos económicos negativos a nivel mundial, las cuales manejaban grandes volúmenes de información y que necesitaban de un ajuste en sus auditorías internas y externas.

  - Las herramientas utilizadas en esta técnica son superiores a las técnicas manuales puesto que evalúan gran cantidad de información en menor tiempo y reducen costos.

- Amplían el alcance de la investigación y permiten realizar pruebas que no pueden efectuarse manualmente, en algunos casos los paquetes permiten la lectura de varios archivos simultáneamente.

- "Esta técnica utiliza herramientas que pueden ser usadas para seleccionar una muestra, analizar las características de una archivo, identificar tendencias en los datos y evaluar la integridad de los mismos".[9]

- Estas herramientas de auditoría generalizadas pueden analizar los datos procesados por muchas aplicaciones, además de elevar la calidad y fiabilidad de las verificaciones realizadas, categorizar y muestrear datos de grandes volúmenes de información para realizar un análisis y ayudar a la toma de decisiones.

✓ **Desventajas**

- Para tener en cuenta uno de los retos a afrontar por las aplicaciones estandarizadas para grandes volúmenes de información se da debido a la gran diversidad de ambientes de procesamiento de información ya que las características de los sistemas varían debido a los diferentes entornos de software y hardware, diferentes estructuras de datos, formatos de registros y funciones de procesamiento, poseen limitantes a la hora de verificar la lógica de procesamiento, para este tipo de aplicaciones es todavía complicado adaptarse a los cambios en los objetivos de la aplicación y otro inconveniente es capacitar a los auditores en el uso del software.

- En caso donde el volumen de información no sea muy amplio los métodos manuales son más efectivos y menos costosos, además algunos tipos de aplicaciones son costosas de desarrollar, implementar y operar.

- **Programas utilitarios y usos generales.** El auditor emplea esta técnica cuando en el proceso de auditoría requiere utilizar diferentes programas los cuales servirán para proteger y salvaguardar la información existente en la empresa.

✓ **Ventajas**

- Es de gran ventaja utilizar esta técnica cuando se trata de manipular una gran cantidad de información y la empresa no cuenta con software especializado para dichas tareas.

- Los programas utilitarios son un aliado efectivo del software operacional, para posibilitar la optimización general de los recursos de informática.

[9] http://www.oracle.com/global/lad/database/audit-vault.html

- El auditor dispone de gran variedad de software general para la realización de tareas básicas de la auditoria tales como la documentación, creación de actas o presentación de informes o resultados. Estas herramientas no proveen una aplicación especializada en el proceso de la auditoría, aún así, considerando el proceso total de auditoría, estas herramientas son igualmente útiles. Entre muchas herramientas se encuentran paquetes de ofimática como Microsoft Office, hojas de cálculo como Excel, lotus 1-2-3, diseñadores de gráficos como Visio, Smart Draw o administradores de correo electrónico como Outlook; con estas herramientas se facilita la creación y administración de documentos, cálculos matemáticos y financieros, creación de diagramas de proceso, organigramas, presentación de gráficos estadísticos etc.

✓ **Desventajas**

- Implica mucha complejidad técnica, puesto que el auditor requiere de mucho conocimiento para poder realizar una evaluación interna de la aplicación.

- Los programas utilitarios podrían fácilmente dañar el sistema, por lo tanto el auditor debe tomar ciertas medidas para evitar pérdida accidental de información y daño en los programas utilizados en la organización.

- Las herramientas utilizadas en esta técnica son muy limitadas en su funcionamiento y alcance con respecto al software hecho a la medida y el software especializado.

- **Software hecho a la medida.** Motivados por alcanzar los estándares de calidad internacional las empresas realizan auditorías internas con el fin de cumplir con los requerimientos exigidos, pero la contratación de un asesor o grupo de asesores conlleva a destinar grande presupuestos para cumplir con las auditorias en las empresas, por tal motivo se han visto en la tareas de realizar software especializados, específicos, hechos a la mediada o software de auditoría con sistemas expertos, permitiendo evaluar la gestión inicial en el tema de calidad, lo cual se refleja en la preparación que presentan a la hora de la realización de la auditoria.

  Permite examinar a las empresas en áreas sistematizadas, en donde se pueden crear o desarrollar programas especiales para la empresa, en este caso el auditor haría las veces de usuario y el área de sistemas la respuesta y la solución a los requerimientos del usuario.

  Existen herramientas de mucha productividad para la auditoria, una de ellas es Groupware “una herramienta especializada que permite a equipos de negocios

trabajar más rápido, compartir más información, comunicarse mas efectivamente, y hacer un mejor trabajo de completamiento de tareas.

Groupware es una forma natural de automatizar el proceso de auditoría. Que usa características de base de datos y procesamiento de flujo de trabajo que pueden ser usados para almacenar e integrar información recolectada y empleada en el proceso de auditoría.

Así como también toman un rol muy importante dentro de la auditoria las herramientas asistidas por computadora CAATs "usadas para evaluar la integridad de una aplicación, determinar la conformidad con procedimientos y monitorear los resultados de procesamientos.

- ✓ **Ventajas**

  - o Actualmente existen diversas técnicas de auditoría, algunas de las cuales permiten un seguimiento y rastreo continuo de las aplicaciones mediante las llamadas rutinas embebidas. Su nombre se debe a que estas son rutinas que se incluyen en el desarrollo de las aplicaciones con el fin de realizar durante el funcionamiento de la aplicación auditada un monitoreo de las diversas transacciones y también se suele incluir un módulo anexo para obtener estadísticas e informes de dichas transacciones. Dado la naturaleza de estas técnicas la información se provee de primera mano, lo cual es una clara ventaja a la hora de realizar los análisis de las transacciones de la aplicación.

  - o Garantiza el cumplimiento de las normas legislativas y de la organización y en cualquier momento es posible ingresar, modificar, eliminar criterios de evaluación de las diferentes modalidades de auditoría existentes, ubicando errores y posibles fraudes, disminuyendo considerablemente el riesgo de no-detección de los problemas.

  - o Leer y comparar los datos de la empresa permitiendo que estos permanezcan intactos para preservar la calidad e integridad, ubicar errores y posibles fraudes, limpiar y normalizar los datos para garantizar la coherencia y los resultados.

  - o Restringe el acceso a la información de la auditoria ya que define usuarios con permisos de ejecución, consulta según su cargo para acceder al sistema.

  - o Satisfacen requerimientos específicos de la auditoria como por ejemplo una rutina de muestreo para la selección de transacciones.

- Ayudan a la administración de la empresa en forma permanente al crear rutinas que realicen tareas de actualización de datos, manejo de base de datos de grandes volúmenes de información.

- No presenta limitaciones relacionales con el lenguaje de consulta que emplea, diseño de procedimientos específicos al sistema informático empleado para el registro de operaciones.

- Permite la verificación de controles de aplicación, tales como: secuencia, integridad, rango, validez fecha.

- Permite organizar datos, consolidarlos y totalizarlos en función de los objetivos perseguidos por el auditor.

- Se puede simular en paralelo los procedimientos a partir de los mismos datos de entrada, para comparar los resultados obtenidos con los ficheros de salida de la aplicación auditada, en la práctica esta herramientas son de gran importancia a la hora de mejorar la evaluación de las áreas examinadas ya que estas permiten realizar pruebas de cumplimiento y pruebas sustantivas, poseen herramientas y gráficos estadísticos, retroalimentan sus bases de conocimiento y presentan informes flexibles y dinámicos.

✓ **Desventajas**

- Conocimiento amplio en lenguajes de programación.

- El desarrollo de rutinas embebidas implica mayor tiempo y costos en el desarrollo de las aplicaciones.

- El hecho de ser software a la medida este no se puede aplicar a otros sistemas ni a otras empresas.

- Dependen en gran medida del sistema actual en uso en la entidad auditada y además necesitan un mantenimiento continuo del sistema para lograr una adaptación a las posibles actualizaciones y cambios del mismo.
- Estos programas y su documentación, deben ser antes revisados por el auditor, para pasar por un proceso de prueba y ensayo en donde se determinara si el software cumple con todas las normas y requerimientos de la empresa.

- **Backup o vaciado de archivos.** La técnica Backup o vaciado de archivos le permite al auditor examinar el contenido de los archivos que se encuentran en el computador, esto se hará mediante una copia o vaciado de archivos en un medio de almacenamiento cualquiera.

✓ **Ventajas**

- Al hacer una Backup de los archivos, el auditor observará detalladamente cada uno de estos, realizando a su vez transacciones, que más adelante se comparan con los archivos originales, permitiendo así, obtener un resultado veraz y efectivo de los datos evaluados.

- Esta técnica es de muy útil para hacer copias de los archivos y como soporte de los centros de PED (Procesamiento electrónico de los datos), evitando una posible destrucción parcial o total de los mismos.

✓ **Desventaja**

- No sería ventajoso emplear esta técnica cuando exista demasiada información, pues aumentaría tiempo y por lo tanto habría retraso en la evaluación.

1.7.6. Técnicas para examinar programas aplicativos

- **Snapshot: Auditoría Operativa y de Sistemas de Información, herramientas de diagnostico en tiempo record. (Imagen Instantánea).** Es una técnica que permite tomar una copia o una fotografía de la memoria de un proceso para llegar a la toma de decisiones en el momento de su actividad. Esta técnica tiene en cuenta los datos de entrada.

  ✓ **Ventajas**

  - Manejar grandes volúmenes de información al permitir tomar una copia de la memoria de un proceso.

  - Maneja instrucciones para reconocer y registrar el flujo de transacciones.

  - Se sigue todo un proceso entre el auditor y los analistas o desarrolladores para llegar al producto final en el cual el auditor recibe toda la documentación de los procesos para finalmente realizar el análisis de los objetivos predefinidos en la auditoria.

  - Manejo de una clave especial para el manejo de la información (datos de entrada).

  - Los snapshots son mucho más rápidos que los backups anteriores ya que solo necesitan trabajar con porciones de datos alteradas.

- Se pueden crear varios snapshots ya que el tamaño en disco es menor a la base de datos original.

- Es más fácil trabajar con snapshots y mucho más rápido para realizar copias de seguridad y restauraciones al sistema.

- Se pueden recuperar datos, eliminados por la snapshot para reparar la base de datos principal.

- Tiene la capacidad de restaurar la base de datos utilizando esta herramienta.

- Facilita al auditor comprender los pasos de procesamiento, verificando el flujo lógico del programa.

✓ **Desventaja**

- La indexación de texto completo no se admite en la Snapshot

- Si los datos de la snapshot cambian en periodos cortos no se lograra una diferencia con los backups tradicionales.

- No se puede deshabilitar la base de datos primaria ya que los snapshot están atados a esta.

- Requiere bastante conocimiento de PED y de programación de computador, consume bastante tiempo.

- **Mapping.** Es una técnica que utiliza una herramienta la cual permite evaluar cada una de las instrucciones de un programa, presentando reportes, tanto del número de veces que es ejecutada una instrucción como el tiempo que duró el procesador en ejecutarlas.

  ✓ **Ventajas**

  - Permite deshabilitar instrucciones ilegales.

  - Identifica instrucciones que no son utilizadas, pues es una técnica segura que sirve como soporte al control de calidad de sistemas para medir eficiencia.

  - Ejecuta procedimiento de depuración de software.

✓ **Desventajas**

- La desventaja es que se requiere de conocimientos avanzados en programación para su desarrollo, consume demasiado tiempo y es costosa.

- **Tracing y Flujograma de control.** El Tracing es una técnica muy importante en cuanto a los lenguajes de programación, puesto que identifica y muestra las instrucciones que fueron ejecutadas y en que secuencia aparecen.

  El flujograma de control es una técnica muy valiosa puesto que permite evaluar los sistemas de una forma integral, tanto en el aspecto funcional como en el de control.

  ✓ **Ventajas**

  - Periódicamente deben ser evaluados ciertos factores o elementos que de una u otra manera brinden confiabilidad al sistema informático, ya que los equipos pueden fallar y producir accidentes informáticos, los errores humanos y los actos intencionales siendo estos los más perjudiciales e importantes.

  - Con el fin de evitar en gran parte se presente este tipo de problemas el sistema debe contar con un componente de identificación de usuarios, asignado roles y permisos de acceso y atribuciones, aquí es donde tracing actúa, verificando a posteriori quienes han ingresado al sistema a qué tipo de información han tenido acceso, que tipo de modificaciones realizaron (fecha, hora, si elimino o modifico información), una gran ventaja a la hora de auditar las entradas al sistema por parte de los usuarios.

  - Tracing obtiene un listado de las transacciones utilizadas, permitiéndole al auditor identificar fácilmente el cumplimiento de los objetivos.

  - Los flujogramas Facilitan la tarea de comparar el funcionamiento manual con el sistema total, verificando que este funcionando de la forma en como están en la documentación.

  - Además los flujogramas de control son excelentes para el entrenamiento de nuevos auditores.

  - El flujograma de control, detecta las deficiencias en materia de control y en el tipo operacional.

- **Comparación de código y control de cambio.** La técnica de comparación de códigos se la utiliza para comparar códigos de una misma versión con el fin de comprobar que estos estén funcionando de una manera correcta.

  Esta técnica debe ser aplicada cuando ya existe un control de cambio, de otra forma se debe buscar alternativas que permitan la búsqueda de la evidencia.

  La técnica de control de cambio es la que verifica el número de bytes de los programas.

  Estas dos técnicas básicamente Impiden que personas infructuosas se sometan a la alteración o cambio de programas, afectando de esta manera a la empresa.

  ✓ **Ventajas**

  - En el control de cambio, evita el aumento de instrucciones perjudiciales para la empresa. Además esta técnica es muy confiable en cuanto a integridad de los programas y respaldando así el contenido de archivos.

  - Una ventaja en cuanto a comparación de código es la de ofrecer mayor seguridad en el cambio de programas y librerías de programas.

  - Se puede obtener una clara identificación del origen de un hallazgo en el código fuente, en qué versión se originó, inclusive, quién estuvo a cargo de dicho cambio.

  ✓ **Desventajas**

  - La técnica de comparación de código no proporciona evidencia sobre confiabilidad de los archivos de datos ni sobre eficiencia de los programas.

  - La desventaja de la técnica de control de cambio es que exige un riguroso sistema de control interno.

  - No es recomendable aplicarla en empresas pequeñas o desarrollos simples, por lo que puede dificultar notablemente la aplicación de dicha técnica, el esfuerzo y recursos necesarios pueden ser excesivos para al final no obtener resultados significativos.

  - Debe existir un historial de versiones. De otra forma no es posible aplicar esta herramienta, ya sea que se lleve control sobre las versiones o comparación de código.

- **Análisis de la lógica del programa.** Esta técnica consiste en evaluar la lógica del programa y el contenido de su documentación de forma descriptiva.

  ✓ **Ventajas**

  - Es la técnica que mejor controla todas las particularidades de un programa.
  - Describe detalladamente un programa.

  ✓ **Desventajas**

  - Seguridad de que la información es una representación exacta de los programas utilizados. Que la documentación no este desactualizada.
  - El auditor debe tener el conocimiento del lenguaje de programación utilizado, para cumplir rápidamente con los objetivos de la auditoria. Que los auditores y revisores fiscales tengan el conocimiento básico en lenguajes de programación para que tengan una buena comunicación con el ingeniero de sistemas o con el experto en el tema.
  - El auditor debe conocer ampliamente todos los sistemas a evaluar para estar al tanto de la forma de la relación entre módulos y programas para tener una mejor comprensión del sistema total.
  - Utilizado únicamente para la evaluación de módulos, porque resulta dificultoso en programas extensos y sofisticados.

2. METODOLOGIA

La metodología utilizada para realizar la auditoria de sistemas al proceso de contratación y las páginas web de las entidades Hospital Universitario Departamental de Nariño E.S.E y al Hospital Civil de Ipiales E.S.E, se rigió por las necesidades emanadas por la Contraloría Departamental de Nariño que a su ves se fundamenta en las facultades otorgadas por la resolución 444 de 2005 Metodología del Proceso Auditor de la Constitución Política.

Este tipo de metodología se enmarca en el tipo de investigación cuantitativa, ya que los resultados finales se obtienen de un proceso de análisis y calificación de tipo numérica de acuerdo a la importancia de distintas variables.

Es responsabilidad de la administración el contenido de la información suministrada por la entidad y analizada por la Contraloría General de Nariño y el equipo auditor conformado por los estudiantes Luis Carlos Chaves Yela y Ricardo Alexander Cabrera Solarte.

La responsabilidad del órgano de control consiste en producir un informe integral que contenga el concepto sobre la gestión adelantada por la administración de la entidad e incluye pronunciamientos sobre el acatamiento a las disposiciones legales y la calidad y eficiencia del Sistema de Control Interno.

De conformidad con lo anterior, se planeó y ejecutó el trabajo de manera que el examen y el resultado de las pruebas proporcionaran una base razonable para fundamentar la opinión y los conceptos expresados en el Informe

Por las características propias de los procesos de auditoría, la metodología que se siguió para cumplir los objetivos propuestos, es de tipo empírico, porque se realiza recolección y análisis de datos, además se toma como fuente primaria de información la observación directa por parte del equipo auditor, también, se estudian y aplican conceptos y esquemas teóricos, también cabe mencionar que esta metodología clasifica dentro del tipo de investigación aplicada, ya que todas las recomendaciones finales deberán ser aplicadas de forma directa e inmediata.

La auditoría realizada por el equipo auditor en compañía del funcionario de la entidad Contraloría Departamental de Nariño fue dividida en varias etapas así:

- **Etapa I. Familiarización con el Entorno.** En esta etapa se realiza el estudio previo al inicio de la Auditoria con el propósito de conocer en detalle las entidades Hospital Universitario Departamental de Nariño E.S.E y el Hospital Civil de Ipiales E.S.E y en si del proceso de contratación que se lleva a cabo en

estas dos entidades, además del tratamiento que se le ha venido dando a la página web como herramienta para el cumplimiento del decreto 1151 de 2008 de Gobierno en Línea.

Los resultados de la exploración permiten, además, hacer la selección de las técnicas y metodologías de auditoría a utilizar.

El equipo auditor se rigió por las normas de auditoría de la entidad Contraloría Departamental de Nariño, se realizaron visitas a las entidades, de las cuales se saco el mayor provecho con la realización de observación directa, además de la aplicación de entrevistas y charlas de carácter formal e informal con los funcionarios de las dos entidades.

- **Etapa II. Planeación de la auditoría de sistemas.** En esta etapa se realizo la planificación de todo el proceso que se requiere para la realización de la auditoría.

  Las actividades que se realizaron dentro de esta etapa fueron:

  - ✓ Identificar el alcance y los objetivos de la Auditoría a realizar.
  - ✓ Realizar el estudio inicial en las entidades Hospital Universitario Departamental de Nariño E.S.E y Hospital Civil de Ipiales E.S.E, para recolectar datos sobre le funcionamiento del proceso de contratación y del cumplimiento del decreto 1151 de 2008 de Gobierno en Línea.
  - ✓ Determinar los recursos necesarios para realizar la auditoría.
  - ✓ Elaboración del plan de trabajo.

- **Etapa III. Realización de las Actividades de la Auditoría.** En esta etapa se hicieron efectivos todos los planteamientos de la etapa anterior, con la aplicación de las metodologías y técnicas escogidas que garantizaron el cumplimiento de los objetivos planeados.

  Las actividades que se realizaron dentro de esta etapa fueron:

  - ✓ Elaboración del plan de auditoría, para identificar dentro de los dominios del COBIT, los procesos y los objetivos de control que se van a evaluar.
  - ✓ Elaboración de los cuadros de definición de fuentes de conocimiento, pruebas de análisis, y pruebas de auditoría, para cada uno de los procesos seleccionados dentro de los dominios del COBIT, para se auditados.

- ✓ Realización de pruebas sobre los procesos seleccionados.

- ✓ Elaboración de los cuestionarios cuantitativos para cada uno de los procesos seleccionados dentro de los dominios del COBIT, para ser auditados.

- ✓ Identificación de hallazgos dentro del proceso evaluado.

- ✓ Asignación de la probabilidad de ocurrencia e impacto para los riesgos detectados mediante la aplicación del formato de hallazgos.

- ✓ Análisis del cumplimiento del decreto 1151 de 2008 de Gobierno en Línea

- **Etapa IV. Presentación del Informe Final.** En esta etapa se realizo el informe final, en donde se describieron los hallazgos encontrados y se hacen las recomendaciones pertinentes para subsanar dichos errores, también se relacionan que partes del proceso de contratación se encuentran sin problemas para que las entidades sepan donde realizar las correcciones del caso, también se produjo el informe donde se indica como elaborar la pagina web para que cumpla con los lineamientos del decreto 1151 de 2008 de Gobierno en Línea.

  Una vez elaborados los informes fueron enviados a la Contraloría Departamental de Nariño para que esta a su ves los haga llegar a las entidades auditadas con el fin de que se presenten las correcciones necesarias.

3. DESARROLLO DEL TRABAJO

3.1. ARCHIVO PERMANENTE

El archivo permanente es la colección de documentos cuya información es valida en el tiempo aunque nos se refiere exclusivamente a un solo periodo.

3.1.1. Leyes y decretos comunes. En este apartado se citaran las leyes y decretos que regularon el proceso de auditoría en las dos entidades.

- **Leyes.** Las leyes que rigen la contratación son los siguientes.

  ✓ Ley 594 del 2000
  ✓ Ley 80 de 1993

- **Decretos.** El decreto que rige los estatutos de conformación de la página web es el siguiente.

  ✓ Decreto 1151 del 2008 de Gobierno en Línea.

3.1.2. Hospital Universitario Departamental de Nariño E.S.E

- **Antecedentes.** El Hospital Universitario Departamental de Nariño E.S.E., es la única organización de la red pública de nivel III de la región, funciona desde el 15 de diciembre de 1975 y en octubre de 1990, mediante Resolución del Ministerio de Salud No.14676.

  El Hospital Departamental de Nariño es clasificado como un organismo para atención de nivel III. A partir del 10 de diciembre de 1994, se constituye en una Empresa social del Estado por ordenanza 067 expedida en la Asamblea Departamental de Nariño, proyectándose con los avances de la Ciencia, la Tecnología y la Gerencia Moderna a la comunidad del Sur Occidente del País.

  Enmarca su accionar actual, circunscrito al entorno del Sistema de la Seguridad Social en Salud, fortaleciendo su estructura organizacional y empresarial frente al reto de este milenio enfocado hacia el III y IV nivel de complejidad.

Actualmente el Hospital Departamental de Nariño E.S.E. cambia su razón social por Hospital Universitario Departamental de Nariño E.S.E.

- **Naturaleza Jurídica.** El Hospital Departamental de Nariño E.S.E. fue creado mediante Ordenanza 067 del 10 de diciembre de 1994 y su estructura organizacional fue modificada con el Acuerdo No 006 del 2004, así como su plan de cargos y de asignaciones fijada mediante Acuerdo 003 del 11 de abril del 2005. Posteriormente, la Asamblea Departamental de Nariño expide la Ordenanza 023 del 17 de diciembre de 2004, donde se cambia la razón social de la empresa, por "Hospital Universitario Departamental de Nariño E.S.E.", esto en procura de fortalecer su parte asistencial, educativa e investigativa.

- **Misión.** "El Hospital Universitario Departamental de Nariño, es una Empresa Social del Estado, que complementa a la Red Departamental de Prestadores de Servicios de Salud en el tercer nivel de complejidad. Creemos y propiciamos el crecimiento integral de nuestro Talento Humano, lo cual nos permite proyectarnos e incidir en el mejoramiento de la salud y calidad de vida de la comunidad del sur occidente colombiano".

- **Visión.** "El Hospital Universitario Departamental de Nariño, dirigirá sus esfuerzos al mejoramiento continuo, se convertirá en una organización centrada en el usuario y fortalecerá la implementación de tecnología de tal manera que complemente de manera armónica la Red de Prestadores de Servicios de Salud en el tercer nivel de complejidad".

- **Valores.** "Nuestros principios trazadores de políticas para el direccionamiento estratégico son: Liderazgo, Servicio al cliente, Trabajo en equipo, Responsabilidad y Conciencia social".

- **Manual de Funciones del Hospital Universitario Departamental de Nariño (Comité de Contratación).** Se transcribió el manual de funciones del comité de contratación extraído del manual de funciones general del Hospital Universitario Departamental de Nariño.

IDENTIFICACION

NIVEL:	DIRECTIVO
DENOMINACIÓN DEL EMPLEO:	GERENTE DE EMPRESA SOCIAL DEL ESTADO
CODIGO:	085
GRADO:	03
NUMERO DE CARGOS:	1
DEPENDENCIA:	GERENCIA
CARGO DEL JEFE INMEDIATO:	JUNTA DIRECTIVA

I. PROPÓSITO PRINCIPAL

Dirección general de la Institución a su cargo, Formulación de políticas institucionales y adopción de planes programas y proyectos de ejecución en la Empresa Social del Estado, ejerciendo labores de dirección, supervisión y control en la administración del hospital, tendientes al logro de la misión y cumplimiento de los objetivos trazados, con visión empresarial, de cubrimiento y calidad en los servicios, en el marco del plan de desarrollo institucional.

II. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Dirigir la empresa, manteniendo la unidad de intereses, en torno a la Misión y Objetivos de la misma de acuerdo a las políticas trazadas en el plan Institucional de gestión y resultados.

2. Realizar la gestión necesaria para lograr el desarrollo de la empresa de acuerdo con los planes y programas establecidos, teniendo en cuenta los perfiles epidemiológicos del área de influencia, las características del entorno y los intereses de la empresa Social.

3. Articular el trabajo que realizan los diferentes niveles de la organización dentro de una concepción participativa de la gestión.

4. Ser nominador y ordenador del gasto de acuerdo con las facultades concedidas por la Ley y los reglamentos.

5. Representar a la Empresa judicial y extrajudicialmente.

6. Velar por el cumplimiento de las Leyes y reglamentos que rigen a las Empresas sociales del Estado.

7. Asistir, Presidir y/o participar en las reuniones de los Consejos, Juntas, Comités y demás cuerpos en que tenga asiento el Hospital y en las demás actividades de la red de servicios en salud o efectuar las delegaciones pertinentes.
8. Adoptar las normas técnicas y legales orientadas a mejorar la prestación de servicios de salud y velar por la validez científica de las técnicas y procedimientos utilizados en el diagnostico y tratamiento.

9. Aplicar de acuerdo a la reglamentación, el sistema de referencia y contra referencia de pacientes.

10. Fomentar el trabajo interdisciplinario y la coordinación intra e intersectorial.

11. Prever la consecución oportuna de los recursos necesarios y promover la utilización racional de los disponibles.

12. Detectar la presencia de todas aquellas situaciones que sean factor de riesgo epidemiológico y adoptar las medidas conducentes a minimizar sus efectos.

13. Desarrollar planes y proyectos de salud conforme a la realidad socio económica y cultural de la región.

14. Participar y lograr la elaboración, y ejecución, del plan de desarrollo Institucional, ejercer control, seguimiento y evaluación al mismo.

15. Velar por la utilización eficiente del recurso humano, técnico y financiero de la entidad y por el cumplimiento de las metas y programas aprobados por la Junta Directiva.

16. Presentar para la aprobación de la Junta Directiva, el plan tribunal, los programas Anuales de desarrollo de la Entidad, el presupuesto prospectivo, de acuerdo con la ley Orgánica del Presupuesto y las normas reglamentarias.

17. Adaptar la entidad a las nuevas condiciones empresariales establecidas en el marco del sistema general de seguridad social en salud, garantizando tanto la eficiencia social como económica de la Entidad, así como competitividad de la Institución.

18. Ejercer control Administrativo para la operatividad del sistema contable y de costos de los servicios, ejecución del presupuesto, recaudación de fondos y propender por la eficiente utilización del recurso financiero.

19. Garantizar el establecimiento del sistema de acreditación hospitalaria, de auditoria en salud y control interno que propicie la garantía de la calidad en la prestación de los servicios de salud.

20. Diseñar y poner en marcha el sistema de información de salud, según las normas Técnicas que expidan el Ministerio de Salud y adoptar los procedimientos para la programación, ejecución, evaluación, control y seguimiento físico y financiero de los programas.

21. Desarrollar objetivos, estrategias y actividades conducentes a mejorar las condiciones laborales, el clima organizacional, la salud ocupacional y el nivel de capacitación y entrenamiento y en especial ejecutar un proceso de educación continuada para todos los funcionarios de la entidad.

22. Presentar a Junta Directiva proyecto de planta de personal y las reformas necesarias para su adecuado funcionamiento y someterlo a la aprobación de la autoridad competente.

23. Nombrar y remover los funcionarios bajo su dependencia de acuerdo con la normas de administración de personal que rigen para las diferentes categorías de empleos, en el Sistema General de Seguridad Social en Salud.

24. Diseñar modelos y metodología para estimular y garantizar la participación ciudadana, propender por la eficiencia de las actividades en las acciones tendientes a lograr metas de salud y el mejoramiento de la calidad de vida de la población.

25. Diseñar mecanismos de fácil acceso a la comunidad, que permitan evaluar la satisfacción de los usuarios, atender las quejas y sugerencias y diseñar en consecuencia, políticas y correctivos orientados al mejoramiento continuo del servicio.

26. Adelantar actividades de transferencia tecnológica, propiciar y desarrollar investigaciones científicas y tecnológicas y promover la realización de pasantías con el fin de ampliar los conocimientos científicos y tecnológicos de los funcionarios del Hospital, con el fin de establecer las causas y soluciones a los problemas de salud.

27. Desarrollar una gestión con calidad y de acreditación utilizando estrategias coherentes de desarrollo organizacional.

28. Velar por la implementación de un sistema de Auditoria de calidad en salud.

29. Velar por el cumplimiento de las Leyes y reglamentos que rige a las Empresa sociales del Estado.

30. Las demás que establezca la Ley, los Reglamentos y la Junta Directiva de la Empresa.

III. CONTRIBUCIONES INDIVIDUALES

1. La empresa se dirige manteniendo la unidad de intereses, en torno a la Misión y Objetivos de la misma de acuerdo a las políticas trazadas en el plan Institucional de gestión y resultados.

2. La empresa se desarrolla respondiendo a los planes y programas establecidos, teniendo en cuenta los perfiles epidemiológicos del área de influencia, las características del entorno y los intereses de la empresa Social.

3. El trabajo que realizan los diferentes niveles de la organización es articulado dentro de una concepción participativa de la gestión.

4. La nominación y ordenación del gasto se realiza considerando las facultades concedidas por la Ley y los reglamentos.

5. La empresa es representada judicial y extrajudicialmente de manera oportuna y diligente.

6. La empresa responde al cumplimiento de las Leyes y reglamentos que rigen este tipo de instituciones prestadoras del Servicio de Salud.

7. En los Consejos, Juntas, Comités y demás cuerpos en que tiene asiento el Hospital asiste, preside y/o participa o efectúa las delegaciones correspondiendo de manera respetuosa, oportuna y diligente.

8. Las normas técnicas y legales orientadas a mejorar la prestación de servicios de salud son adoptadas de manera oportuna coordinando con los grupos de trabajo involucrados.

9. Las técnicas y procedimientos utilizados en el diagnostico y tratamiento se validan científicamente mediante reuniones con el Comité Científico y la participación de los Coordinadores de los Grupos Internos de Trabajo.

10. El sistema de referencia y contra referencia de pacientes responde a la reglamentación vigente que regula la materia.

11. El trabajo interdisciplinario y la coordinación intra e intersectorial es fomentado a través de los diferentes Comités establecidos en el Hospital y los Coordinadores de los Grupos Internos de Trabajo.

12. Los recursos necesarios se consiguen oportunamente siguiendo los criterios de oportunidad y razonabilidad.

13. Los recursos necesarios son utilizados respondiendo a una política de promoción de su utilización racional que se realiza por medio de las Subgerencias y los Coordinadores de los Grupos Internos de Trabajo.

14. Las situaciones que sean factor de riesgo epidemiológico son detectadas oportunamente y se adoptan las medidas conducentes a minimizar sus efectos.

15. Los planes y proyectos de salud son desarrollados considerando a la realidad socio económica y cultural de la región.

16. Participar y lograr la elaboración, y ejecución. El plan de desarrollo Institucional es aprobado, seguido y evaluado, mediante su participación activa y en compañía de las Subgerencias y los Coordinadores de los Grupos Internos de Trabajo.

17. El recurso humano, técnico y financiero de la entidad responde a criterios de utilización eficiente y siguiendo las normas legales vigentes y el cumplimiento de las metas y programas aprobados por la Junta Directiva.

18. El plan tribunal, los programas Anuales de desarrollo de la Entidad, el presupuesto prospectivo, son presentados a la Junta Directiva siguiendo las directrices de la ley Orgánica del Presupuesto y las normas reglamentarias.

19. Las condiciones empresariales establecidas en el marco del sistema general de seguridad social en salud son adaptadas garantizando tanto la eficiencia social como económica de la Entidad, así como competitividad de la Institución.

20. El control administrativo para la operatividad del sistema contable y de costos de los servicios, ejecución del presupuesto, recaudación de fondos es ejercido propendiendo por la eficiente utilización del recurso financiero es ejercido

21. El sistema de acreditación hospitalaria, de auditoria en salud y control interno es garantizado con el fin de propiciar la garantía de la calidad en la prestación de los servicios de salud.

22. El sistema de información de salud es diseñado y puesto en marcha según las normas Técnicas que expidan el Ministerio de Salud.

23. Los procedimientos para la programación, ejecución, evaluación, control y seguimiento físico y financiero de los programas son adoptados siguiendo la normatividad legal vigente.

24. Los objetivos, estrategias y actividades conducen a mejorar las condiciones laborales, el clima organizacional, la salud ocupacional y el nivel de capacitación y entrenamiento.

25. El proyecto de planta de personal y las reformas necesarias para su adecuado funcionamiento es sometido a la Junta Directiva teniendo en cuenta los estudios técnicos y la normatividad legal vigente.

26. Los funcionarios bajo su dependencia son nombrados y removidos de acuerdo con la normas de administración de personal que rigen para las diferentes categorías de empleos, en el Sistema General de Seguridad Social en Salud.

27. La participación ciudadana es diseñada siguiendo modelos y metodologías que propenden por la eficiencia de las actividades en las acciones tendientes a lograr metas de salud y el mejoramiento de la calidad de vida de la población.

28. Los mecanismos de acceso a la comunidad son diseñados de manera que permiten evaluar la satisfacción de los usuarios, atender las quejas y sugerencias y diseñar en consecuencia, políticas y correctivos orientados al mejoramiento continuo del servicio.

29. Las actividades de transferencia tecnológica son adelantadas considerando factores de referenciación competitiva.

30. La investigación científica, tecnológica y las pasantías se promocionan, respaldan y promueven con el fin de ampliar los conocimientos científicos y tecnológicos de los funcionarios del Hospital.

31. La gestión con calidad y de acreditación responde a estrategias coherentes de desarrollo organizacional.

32. El sistema de Auditoria de calidad en salud es implementado siguiendo las normas técnicas y jurídicas vigentes en la materia.

33. Las Leyes y reglamentos que rige a las Empresa sociales del Estado son respetadas como criterios orientadores de la gestión.

IV. CONOCIMIENTOS BÁSICOS O ESENCIALES

• Metodología de investigación y desarrollo de proyectos

• Plan de Desarrollo organizacional

• Plan Nacional de Capacitación

• Normas sobre administración de personal

V. REQUISITOS DE ESTUDIO O EXPERIENCIA

A. EDUCACION: Título de Profesional en Ciencias de la Salud, Economía, Administración de Empresas, Derecho, con tarjeta Profesional.

B. FORMACIÓN: Título de formación avanzada o Postgrado en Salud Pública, Administración en salud, Gerencia hospitalaria o en áreas económicas o administrativas afines.

C. EXPERIENCIA: Experiencia profesional de cuatro (4) años en empleos de nivel Directivo, Asesor, Ejecutivo o Profesional en organismos o entidades públicas o privadas que integran el Sistema General de Seguridad Social en Salud.

IDENTIFICACIÓN

NIVEL:	DIRECTIVO
DENOMINACIÓN DEL EMPLEO:	SUBGERENTE
CODIGO:	090
GRADO:	01
NUMERO DE CARGOS:	1
DEPENDENCIA:	SUBGERENCIA DE PRESTACION DE SERVICIOS
CARGO DEL JEFE INMEDIATO:	GERENTE DE EMPRESA SOCIAL DEL ESTADO

I. PROPOSITO PRINCIPAL

Prestar servicios Gerenciales a la Empresa, adoptando las políticas institucionales, mediante la realización de procesos de dirección, organización, planeación y control, de la producción de los servicios de salud definido en el portafolio de la Empresa, garantizando el logro de la Misión social y financiera de la E.S.E., a partir del logro de los objetivos de cada una de las unidades orgánicas de producción de servicios.

II. DESCRIPCIÓN DE FUNCIONES ESENCIALES.

1. Contribuir con el logro de la misión y los objetivos de la Empresa, a través de Garantizar cumplimiento de la finalidad del Área de prestación de servicios y de cada una de sus secciones, tanto en la perspectiva de la eficiencia y calidad de los servicios, para el logro de beneficios sociales como en la perspectiva de la rentabilidad financiera.

2. Elaborar el programa de actividades médicas del Hospital a fin de garantizar una adecuada organización en la prestación de los servicios que demanden las necesidades de la comunidad

3. Dirigir la producción de servicios de Salud por la Empresa, a través de sus diferentes secciones, coordinando e integrando acciones y estableciendo mecanismos de control del personal bajo su dependencia.

4. Liderar la labor de los coordinadores de unidad y coordinadores administrativos, para la prestación de servicios, quienes son los responsables de la producción en cada uno de las unidades de servicios del hospital, vigilando que cada uno asuma sus responsabilidades de conformidad con las directrices de la Junta Directiva y de la Gerencia.

5. Fomentar el trabajo interdisciplinario, estableciendo, ejerciendo y manteniendo, los mecanismos de coordinación necesarios para la unificación de criterios para la prestación de servicios, con sentido de pertenencia, en la perspectiva de lograr posicionamiento de la Entidad en la prestación de los servicios en salud.

6. Mediante la formulación de un portafolio de servicios prestados por la Empresa a través de cada una de las secciones, organizar la producción de los servicios que esta ofrece, definiendo e integrando los procesos a realizar, servicios a producir y los clientes a satisfacer.

7. Planear la producción de los servicios de la Empresa, liderando e integrando la elaboración del Plan Operativo Anual de Negocios (POA) en cada una de las Secciones y la Programación anual de los servicios de acuerdo con los requerimientos y necesidades de los usuarios.

8. Ejercer el control y evaluación de la producción de servicios liderando la implementación de un sistema de información gerencial que le permita realizar, en conjunto con los coordinadores un control y seguimiento de la gestión de producción.

9. Velar porque la Empresa satisfaga las necesidades de recursos requeridos para la producción de servicios, manteniendo la integración y coordinación de acciones con la Gerencia, la Subgerencia Administrativa y los coordinadores de apoyo administrativo y logístico.

10. Identificar y procurar la disponibilidad de recurso médico especializado en cada una de las unidades y dirigir su actividad, tanto productiva como científica. Siendo el responsable directo de la programación, dirección y control de este recurso.

11. Implementar los principios y las acciones tendientes a mejorar la calidad de la prestación de los servicios dentro del marco del sistema de seguridad social en salud, en concordancia con los coordinadores de unidad y los Coordinadores Administrativos.

12. Contribuir con la oficina de Auditoria Médica para la formulación de los principios, procedimientos y técnicas para realizar el control verificativo de procesos y procedimientos técnico científico y el cumplimiento de las normas técnicas y legales.

13. Liderar la realización de actividades de vigilancia y control epidemiológico, en coordinación con el Comité de Vigilancia Epidemiológica.

14. Coordinar la implementación y puesta en funcionamiento de los comités técnico científica y administrativa, que se requieran para la adecuada prestación de servicios.

15. Convenir, coordinar, controlar, las actividades docente asistenciales que de cualquier nivel se requieran y soliciten, procurando equidad de beneficios.

16. Participar en las acciones que sean necesarias para propiciar el avance científico de los procesos de prestación de servicios de salud en la entidad y apoyar el desarrollo de actividades de investigación tendientes a desarrollar la identificación, prevención, tratamiento y control de las enfermedades, y el desarrollo de los procesos administrativos y Gerenciales de prestación de servicios.

17. Desempeñar las demás funciones asignadas que sean afines a la naturaleza del cargo y lo prescriban las normas.

III. CONTRIBUCIONES INDIVIDUALES.

1. Garantizando el cumplimiento del área de prestación de servicios y de cada una de sus secciones, tanto en la perspectiva de la eficiencia y calidad de los servicios se contribuirá con el logro de la misión y los objetivos de la Empresa.

2. Garantizando una adecuada organización en la prestación de los servicios que demanden las necesidades de la comunidad elaborando el programa de actividades médicas del Hospital.

3. Asumir el liderazgo en la labor de los coordinadores de Unidad para la prestación de servicios vigilando que cada uno asuma sus responsabilidades.

4. Estableciendo mecanismos de Coordinación necesarios para la unificación de criterios en la prestación de servicios con sentido de pertenencia, fomentando el trabajo interdisciplinario.

5. Organizar la producción de los servicios mediante la presentación de un portafolio de servicios prestado por la Empresa definiendo e integrando los procesos para satisfacer las necesidades de los clientes

6. Liderar, e integrar la elaboración del plan operativo anual de negocios en cada una de las secciones.

7. Realizar conjuntamente con los coordinadores un control y seguimiento a la gestión de producción.

8. Dirigir la actividad tanto productiva como científica y procurar la disponibilidad del recurso médico especializado en cada una de las unidades.

9. Formular los principios, procedimientos y técnicas para realizar el control verificativo de procesos y procedimientos técnicos científicos y el cumplimiento de las normas técnicas y legales conjuntamente con Auditoria Médica.

10. Liderar los comités de vigilancia y control epidemiológico, técnico científico, de historias clínicas de ética médica.

11. Se coordinarán y controlaran las actividades docentes asistenciales.

12. Interactuar con los diferentes actores de la prestación de servicios para satisfacer las necesidades el cliente y dirimir conflictos.

IV. CONOCIMIENTOS BÁSICOS O ESENCIALES

- Ley 100 de 1993
- Decreto 1011 Sistema Obligatorio de Garantía de la Calidad
- Normas ISO – 9001 / 2000
- Normas que regulan el funcionamiento y atención a usuarios del régimen contributivo, subsidiado, subsidiado parcial, población vinculada, desplazados, enfermedades catastróficas y accidentes de transito.
- Acuerdo 228) medicamentos POS)
- Resolución 1995.
- Decreto 2423 Manuel Tarifario SOAT
- Manual Tarifario ISS
- Normas Para facturación de servicios de salud

V. REQUISITOS DE ESTUDIO O EXPERIENCIA

A. EDUCACION: Titulo Profesional en Ciencias de la Salud.

B. FORMACIÓN: Título en Formación Avanzada o Postgrado en Gerencia de Servicios de salud, Seguridad Social en Salud, Gerencia Hospitalaria o en otras áreas afines con la salud.

C. EXPERIENCIA: Tres (3) años de experiencia Profesional, en cargos Directivos o de Asesoría relacionados con el cargo.

IDENTIFICACIÓN

NIVEL:	DIRECTIVO
DENOMINACIÓN DEL EMPLEO:	SUBGERENTE
CODIGO:	090
GRADO:	01
NUMERO DE CARGOS:	1
DEPENDENCIA:	SUBGERENCIA ADMINISTRATIVA Y FINANCIERA
CARGO DEL JEFE INMEDIATO:	GERENTE DE EMPRESA SOCIAL DEL ESTADO

I. PROPOSITO PRINCIPAL

Prestar servicios Gerencial a la Empresa, mediante la realización de procesos de dirección, organización, planeación y control, liderando la gestión empresarial de prestación de servicios de administración de recursos y de apoyo logístico necesarios para el logro de la Misión social y financiera de la ESE.

II. DESCRIPCIÓN DE FUNCIONES ESENCIALES.

1. Contribuir a alcanzar la finalidad de la Empresa, a través del cumplimiento de las metas del Área Administrativa y de Apoyo Logístico y de cada una de sus secciones, tanto en la perspectiva de la rentabilidad social como de la rentabilidad financiera.

2. Atender las actividades relacionadas con la adquisición, almacenamiento y suministro de elementos, materiales y equipos que requieran las diferentes dependencias.

3. Planear, controlar evaluar y ajustar los mecanismos administrativos necesarios para el normal funcionamiento del Hospital Departamental de Nariño E.S.E.

4. Dirigir y controlar el archivo general de documentos.

5. Liderar la labor de los coordinadores, quienes son los responsables de brindar el apoyo administrativo para la producción de servicios, vigilando que cada uno asuma sus responsabilidades de conformidad con las directrices de la Junta Directiva y de la Gerencia.

6. Fomentar el trabajo interdisciplinario, estableciendo, ejerciendo y manteniendo, los mecanismos de coordinación necesarios para la unificación de criterios.

7. Facilitar la consecución oportuna de los recursos y herramientas de trabajo y promover la utilización racional de los disponibles.
8. Coordinar, ordenar y analizar la elaboración del Presupuesto de Rentas y Gastos, la adecuada ejecución del mismo y establecer el impacto en la relación costo/ beneficio.

9. Formular la estrategia de mercado de los servicios de salud que satisfaga las necesidades de los usuarios e implementar las acciones correspondientes.

10. Analizar la información estadística generada en la prestación de servicios, como los estados financieros y ejecuciones de presupuesto, para una eficaz toma de decisiones administrativas.

11. Planear las actividades administrativas de la empresa, liderando la elaboración de programación de actividades en cada una de las Secciones bajo su dependencia.

12. Velar porque la Empresa satisfaga las necesidades de recursos requeridos para la producción de servicios, manteniendo la integración y coordinación de acciones con la Gerencia, la Subgerencia de Prestación de Servicios y los coordinadores.

13. Velar por la aplicación de las políticas de selección, control y bienestar del Talento Humano del Hospital.

14. Controlar y lograr la oportunidad y calidad de la información, para dar cumplimiento a los reportes, informes y las obligaciones contraídas.

15. Coordinar la implementación y puesta en funcionamiento de los comités administrativos, que se requieran para la adecuada prestación de servicios.

16. En coordinación con las unidades de prestación de servicios y las administrativas, establecer y hacer la programación financiera del recurso humano, de los suministros, de la información y de los servicios logísticos.

17. Liderar la implementación de un sistema de información Gerencial que le permita realizar, en conjunto con los coordinadores un control de la gestión de sus procesos.

18. Garantizar junto con la Gerencia, la realización de las negociaciones entre la Empresa y las entidades de aseguramiento del sistema, realizando los estudios previos correspondientes, de orden financiero, técnico y legal, prestando todo el apoyo de información y asesoría necesario para la negociación.

19. Coordinar y controlar el suministro de servicios generales, como mantenimiento, vigilancia y demás que se requieran para el correcto funcionamiento de la Institución.

20. Presentar los informes que le sean solicitados sobre el desarrollo de sus funciones.

21. Desempeñar las demás funciones asignadas y que sean afines al propósito principal

III. CONTRIBUCIONES INDIVIDUALES

1. La finalidad de la Empresa, a través del cumplimiento de las mestas del Área Administrativa y de Apoyo, tanto en la perspectiva de la rentabilidad social como de la rentabilidad financiera, responde a la contribución oportuna y eficaz de la Subgerencia.

2. La aprobación de elementos, materiales y equipos se atiende manera oportuna y respetando el principio de racionalidad.

3. Los mecanismos administrativos necesarios para el normal funcionamiento del Hospital Universitario Departamental de Nariño E.S.E. responden a una planeación, control, evaluación y ajuste soportados en un proceso de mejoramiento continúo.

4. El archivo general de documentos es dirigido y controlado siguiendo las normas técnicas aplicables para ello.

5. La labor de los coordinadores del área administrativa es liderada respondiendo a los intereses de la institución encaminados a alcanzar el cumplimiento de los objetivos institucionales.

6. Las responsabilidades de los coordinadores del área administrativa es vigilada de conformidad con las directrices de la Junta Directiva y de la Gerencia.

7. El trabajo interdisciplinario, es fomentado respondiendo a los mecanismos de coordinación necesarios para unificar criterios

8. La consecución y utilización de los recursos y herramientas de trabajo responde a los criterios de oportunidad y racionalidad.

9. El presupuesto de Rentas y Gastos se coordinar, ordena y analiza, respondiendo al cumplimiento de las normas presupuestales vigentes.

10. Las estrategia de mercado en que acompaña a la Subgerencia de Prestación de Servicios son realizadas buscando el beneficio social y la sostenibilidad financiera.

11. La información estadística analizada, los estados financieros y ejecuciones de presupuesto, analizados permite una eficaz toma de decisiones administrativas.

12. Las actividades administrativas de la empresa son planeadas de forma tal que permiten la programación de actividades en cada una de las áreas bajo su dependencia.

13. Las necesidades de recursos son realizadas velando por la integración y coordinación de acciones con la Gerencia, la Subgerencia de Prestación de Servicios y los coordinadores.

14. Las políticas de selección, control y bienestar del talento humano son realizadas velando para que éstas cumplan sus objetivos básicos.

15. La oportunidad y calidad de la información, responde a dar cumplimiento a los reportes, informes y las obligaciones contraídas.

16. La puesta en funcionamiento de los comités administrativos, se coordina bajo la implementación del modelo de gestión de calidad.

17. El establecimiento de la programación financiera del recurso humano, de los suministros de la información, de los servicios logísticas se realiza en coordinación con las unidades de prestación de servicios y administrativas.

18. La implementación de un sistema de información gerencial, se realiza teniendo presente las motivaciones de los diferentes coordinadores en lograr un control de gestión de sus procesos.

19. La realización de las negociaciones entre la empresa y las entidades de aseguramiento del sistema, se garantizan realizando los estudios previos del orden financiero, técnico y legal.

20. El suministro de los insumos para los servicios generales, se coordina y controla con coordinadores de las áreas con el fin de lograr una efectiva realización del gasto.

21. Los informes solicitados son entregados en forma oportuna y correspondiendo a las funciones del cargo

IV. CONOCIMIENTOS BÁSICOS O ESENCIALES

- Conocimientos básicos de la Administración Hospitalaria.
- Conocimientos básicos de la Administración Pública.
- Conocimientos básicos de la Ley Orgánica de Presupuesto.
- Conocimiento de las normas y requisitos de la contabilidad general
- Conocimiento básico del Código Único Disciplinario.
- Conocimiento del Sistema General de Seguridad Social.

V. REQUISITOS DE ESTUDIO O EXPERIENCIA

A. EDUCACION: Título Profesional en Economía, Administración de Empresas, Ingeniería Industrial, Derecho.

B. FORMACIÓN: Título de Formación Avanzada o Postgrado en Salud Pública, Finanzas, Administración Pública, Administración o Gerencia de negocios o de Servicios en Salud.

C. EXPERIENCIA: Tres (3) años de experiencia Profesional, en cargos Directivos o Administrativos.

IDENTIFICACIÓN

NIVEL:	ASESOR
DENOMINACIÓN DEL EMPLEO:	JEFE OFICINA ASESORA
CODIGO:	115
GRADO:	03
NUMERO DE CARGOS:	1
DEPENDENCIA:	OFICINA ASESORA JURÍDICA
CARGO DEL JEFE INMEDIATO:	GERENTE DE EMPRESA SOCIAL DEL ESTADO

I. PROPOSITO PRINCIPAL

Ejercer labores de Asesoría y Asistencia Jurídica a los funcionarios del Nivel Directivo, asumiendo funciones de representación judicial o extrajudicial en cumplimiento de los poderes que le sean otorgados legalmente por el Gerente del Hospital Departamental de Nariño.

II. DESCRIPCIÓN DE FUNCIONES ESENCIALES.

1. Asesorar a las Directivas y demás personal del Hospital Departamental de Nariño ESE. en los asuntos jurídicos y legales relacionados con las funciones y actividades que son propias a sus cargos.

2. Asistir al nivel Directivo del Hospital Departamental de Nariño ESE en la realización de estudios de carácter legal y asuntos procesales.

3. Preparar, revisar y conceptuar sobre los proyectos de resolución, órdenes de trabajo, ordenes de servicio, pliegos de condiciones, sin detrimento de la función que en este sentido le corresponda a otra dependencia.

4. Orientar en los procesos de contratación;

5. Atender los litigios en que sea parte el Hospital Departamental de Nariño ESE y adelantar las gestiones que estos requieran.

6. Asesorar, orientar y coordinar jurídicamente el proceso y trámite de la contratación estatal, aplicando las normas estatutarias y la reglamentación aplicable en la materia y las del sector de prestación de servicios en Salud, con el fin de asegurar que el Hospital se ajuste a la ley en los negocios que adelante.

7. Dirigir y coordinar la compilación y actualización de la legislación y jurisprudencia, relativas a las actividades y funciones de establecimientos

hospitalarios y específicamente Empresas Sociales del Estado. Actualizando permanentemente las normas internas de la Empresa de acuerdo a las normas legales vigentes.

8. Conocer, intervenir, vigilar y mantener actualizado el estado de las demandas instauradas en contra y por del Hospital Departamental de Nariño E.S.E., y por el cumplimiento de lo estipulado en la contratación que mantenga el Hospital, haciendo efectivos las cláusulas contenidas en los mismos

9. Participar y presentar propuestas de carácter jurídico en los comités en que se requiera su presencia y colaborar con la oficina de Control Interno Disciplinario sobre los procesos que se adelanten en la Empresa.

10. Atender las novedades de tipo legal en que tenga que solicitar o dar respuesta el Hospital, como: tutelas, peticiones, reclamaciones; así mismo asistir al Gerente del Hospital en los actos conciliatorios.

11. Desempeñar las demás funciones señaladas en la Constitución, la Ley y demás disposiciones asignadas y que sean afines con la naturaleza del cargo.

III. CONTRIBUCIONES INDIVIDUALES

1. Las Directivas y demás personal del Hospital Departamental de Nariño ESE. Asesorados en los asuntos jurídicos y legales relacionados con las funciones y actividades que son propias a sus cargos reciben oportunamente la asesoría.

2. Las Directivas y demás personal del Hospital Departamental de Nariño ESE asesorado en los asuntos jurídicos y legales relacionados con las funciones y actividades que son propias a sus cargos reciben asesoría fundamentada en las normas legales vigentes, la jurisprudencia y la doctrina.

3. Los estudios de carácter legal y asuntos procesales realizados con el fin de asistir al nivel Directivo del Hospital Departamental de Nariño ES, se soportan en la normatividad vigente, la jurisprudencia, la doctrina y los demás criterios auxiliares del derecho.

4. Los proyectos de resolución, órdenes de trabajo, órdenes de servicio, pliegos de condiciones, son preparados, revisados y objeto de concepto y se ajustan a la normatividad legal vigente.

5. Los procesos de contratación orientados se realizan adecuadamente siguiendo las pautas que dicta el Estatuto Interno de Contratación y demás normatividad legal vigente, la jurisprudencia, la doctrina y los demás criterios auxiliares del derecho.

6. Los litigios en que es parte el Hospital Universitario Departamental de Nariño E.S.E. son atendidos con diligencia y oportunidad, bajo el principio de que su función es de gestión y no de resultado.

7. Los procesos y el trámite de la contratación estatal son asesorados y orientados jurídicamente aplicando las normas estatutarias y la reglamentación aplicable en la materia, la jurisprudencia, la doctrina y demás criterios auxiliares del derecho.

8. Los negocios que adelanta el Hospital Universitario Departamental de Nariño E.S.E. están ajustados a la normatividad vigente.

9. La legislación y jurisprudencias relativas a las actividades y funciones de establecimientos hospitalarios y específicamente a las Empresas Sociales del Estado son compilados y actualizados de forma sistemática y organizada.

10. Las normas internas del Hospital Universitario Departamental de Nariño E.S.E. son actualizadas de forma permanente y organizada.

11. Las demandas instauradas contra y por el Hospital Universitario Departamental de Nariño E.S.E. son conocidas, vigiladas e intervenidas siguiendo los criterios éticos que regulan la profesión de abogado.

12. Los contratos estatales y la efectividad de las cláusulas contenidas en los mismos son conocidas, vigiladas y ejecutadas según los procedimientos señalados en la normatividad legal vigente, el Estatuto Interno de Contratación, la jurisprudencia, la doctrina y demás criterios auxiliares del derecho, o según los procedimientos que se indiquen en los contratos.

13. Las propuestas de carácter jurídico son presentadas en los comités donde se requiere su presencia.

14. Las propuestas de carácter jurídico responde a la normatividad legal vigente, la jurisprudencia y la doctrina, y los demás criterios auxiliares del derecho.

15. Las propuestas de carácter jurídico responden a los parámetros éticos que regulan la profesión de abogado.

16. La colaboración brindada a la oficina de Control Interno Disciplinario sobre los procesos que se adelanten en el Hospital Universitario Departamental de Nariño E.S.E. responden a la normatividad legal vigente, la jurisprudencia y la doctrina, y los demás criterios auxiliares del derecho.

17. La colaboración brindada a la oficina de Control Interno Disciplinario sobre los procesos que se adelanten en el Hospital Universitario Departamental de Nariño

ESE. Responden a los parámetros éticos que regulan la profesión de abogado y no se inmiscuyen en la independencia de la función disciplinaria.

18. Las novedades de tipo legal en que tenga que solicitar o dar respuesta el Hospital, como: tutelas, peticiones, reclamaciones; así mismo asistir al Gerente del Hospital en los actos conciliatorios se atienden oportunamente de acuerdo a los plazos legales preestablecidos.
19. Las novedades de tipo legal en que tenga que solicitar o dar respuesta el Hospital, como: tutelas, peticiones, reclamaciones; así mismo asistir al Gerente del Hospital en los actos conciliatorios responden a la normatividad legal vigente, la jurisprudencia y la doctrina, y los demás criterios auxiliares del derecho.

20. Las novedades de tipo legal en que tenga que solicitar o dar respuesta el Hospital, como: tutelas, peticiones, reclamaciones; así mismo asistir al Gerente del Hospital en los actos conciliatorios responden a los parámetros éticos que regulan la profesión de abogado.

IV. CONOCIMIENTOS BÁSICOS O ESENCIALES

• Normas, jurisprudencia y doctrina sobre Derecho Administrativo General.

• Normas, jurisprudencia y doctrina sobre Derecho Laboral Administrativo.

• Normas, jurisprudencia y doctrina sobre Contratación Estatal.

• Ley 100 de 1.993 y Decretos Reglamentarios, jurisprudencia y doctrina.

• Normas, jurisprudencia y doctrina sobre el Seguro de Accidentes de Tránsito.

• Normas, jurisprudencia y doctrina sobre Derecho Comercial.

• Normas, jurisprudencia y doctrina sobre manejo de Presupuesto Público.

• Normas, jurisprudencia y doctrina sobre Derecho Disciplinario y Penal

• Normas, jurisprudencia y doctrina sobre Derecho Penal.

V. REQUISITOS DE ESTUDIO O EXPERIENCIA

A. EDUCACION: Título Profesional en Derecho, con Tarjeta Profesional vigente.

B. FORMACIÓN: Titulo de Formación Avanzada o de Postgrado en áreas relacionadas con el cargo.

C. EXPERIENCIA: Tres (3) años de experiencia Profesional, relacionadas con las funciones del cargo o de Asesoría.

IDENTIFICACIÓN

NIVEL:	ASESOR
DENOMINACIÓN DEL EMPLEO:	ASESOR
CODIGO:	105
GRADO:	3
NUMERO DE CARGOS:	1
DEPENDENCIA:	OFICINA CONTROL INTERNO DE GESTION
CARGO DEL JEFE INMEDIATO:	GERENTE DE EMPRESA SOCIAL DEL ESTADO

I. PROPOSITO PRINCIPAL

Ejecución de labores de Asesoría, prestando servicios específicos de generar una cultura de auto control en apoyo a la labor del Gerente, del equipo de Gerencia y de la Empresa en su conjunto, realizando procesos de evaluación permanente, eficiente, integral y oportuna, planificación y aplicación del sistema de control interno de la Empresa y proponer al Gerente las decisiones requeridas para mantener o modificar la situación.

II. DESCRIPCIÓN DE FUNCIONES ESENCIALES.

1. Liderar, planear, organizar y evaluar el Sistema de Control Interno ejercido por los funcionarios.

2. Verificar que el sistema de control interno esté formalmente establecido dentro de la Empresa y que su ejercicio sea intrínseco al desarrollo de las funciones de todos los cargos y, en particular, de aquellos que tengan responsabilidad de mando.

3. Verificar que los controles definidos para los procesos y actividades de la organización, se cumplan por los responsables de su ejecución.

4. Verificar que los controles asociados en todas y cada una de las actividades de la Empresa, estén adecuadamente definidos, sean apropiados y se mejoren permanentemente, de acuerdo con la evolución de la institución.

5. Velar por el cumplimiento de las leyes, políticas, misión objetivos, planes, programas, proyectos, metas y procedimientos de la organización y recomendar al Gerente los ajustes necesarios.

6. Servir de apoyo a los Directivos en el proceso de toma de decisiones, a fin de que se obtengan los resultados esperados.

7. Verificar los procesos relacionados con el manejo de los recursos, bienes y los sistemas de información de la entidad y recomendar al Gerente los correctivos que sean necesarios.

8. Fomentar en toda la organización la formación de una cultura del Autocontrol que contribuya al mejoramiento continuo en el cumplimiento de la misión de la Empresa.

9. Evaluar y verificar la aplicación de los mecanismos de participación ciudadana que, en desarrollo del marco constitucional y legal, diseñe la Empresa

10. Mantener permanentemente informados a los Directivos de la Empresa, cerca del estado del Control Interno en la entidad, dando cuenta de las debilidades detectadas y las fallas en su cumplimiento.

11. Verificar que se implanten las medidas recomendadas.

12. Prestar servicios de control ejecutivo o control de la gestión empresarial, con el fin de generar una retroalimentación acerca del comportamiento de los mismos, mediante reportes y recomendaciones tanto de carácter general de la Empresa como específicos por dependencias.

13. Identificar los procesos, productos y clientes, al igual que los requerimientos de información y puntos de control de los procesos, definiendo los estándares o rangos de normalidad del desempeño de los procesos, elaborando instrumentos de medición de acuerdo con las fuentes de la información y realizar un análisis con la situación encontrada.

14. Prestar servicios de control evaluativo o control de los objetivos y metas del plan de desarrollo institucional, con el fin de generar una retroalimentación acerca del comportamiento de los mismos mediante reportes y recomendaciones tanto de los objetivos corporativos como de las metas de las dependencias.

15. Prestar servicios de control verificativo o de auditoria administrativa de los procedimientos propios de los procesos de la Empresa en cualquiera de sus dependencias, con el fin de generar una retroalimentación acerca del comportamiento de los mismos mediante reportes y recomendaciones dirigidos a los responsables de los procesos del nivel Directivo y a los actores de los mismos.

16. Identificar, mejorar y/o facilitar la elaboración de los Manuales de Procedimientos de los procesos de la ESE basados siempre en los requerimientos de orden legal y/ o técnico que se especifiquen y requieran.

17. Diseñar instrumentos de recolección de información para la verificación y contrastar la información encontrada con los manuales donde se ha normalizado, estandarizado y mejorado el funcionamiento.
18. Las demás que le asigne el Gerente de acuerdo con la naturaleza de sus funciones.

III. CONTRIBUCIONES INDIVIDUALES

1. La evaluación y verificación en forma independiente y objetiva del Control Interno Contable es eficaz, al igual que la información transmitida al representante legal de la entidad, sobre las medidas que permitan el mejoramiento continuo del Sistema.

2. Liderar y garantizar que la planeación, organización y evaluación del Sistema de Control Interno ejercido por los funcionarios es el adecuado.

3. Asegura que el Sistema de Control Interno esté formalmente establecido dentro de la Empresa y que su ejercicio sea intrínseco al desarrollo de las funciones de todos los cargos y, en particular, de aquellos que tengan responsabilidad de mando.

4. Verificar que los controles definidos para los procesos y actividades de la organización, se cumplan por los responsables de su ejecución.

5. El cumplimiento de las leyes, políticas, misión objetivos, planes, programas, proyectos, metas y procedimientos de la organización es el adecuado; caso contrario se recomendará al Gerente los ajustes necesarios.

6. Apoya a los Directivos en el proceso de toma de decisiones y Fomenta la organización la formación de una cultura del Autocontrol que contribuya al mejoramiento continuo en el cumplimiento de la misión de la Empresa.

7. Mantiene permanentemente informados a los Directivos de la Empresa, acerca del estado del Control Interno en la entidad.

8. Garantiza que los procesos, productos y clientes, al igual que los requerimientos de información y puntos de control de los procesos son los adecuados al igual que sus instrumentos de medición.

9. Presta servicios de control evaluativo o control de los objetivos y metas del plan de desarrollo institucional, con el fin de generar una retroalimentación acerca del comportamiento de los mismos mediante reportes y recomendaciones tanto de los objetivos corporativos como de las metas de las dependencias.

10. Facilita la elaboración de los Manuales de Procedimientos de los procesos del Hospital basados siempre en los requerimientos de orden legal y/ o técnico que se especifiquen y requieran.

11. Determina el nivel de cumplimiento de leyes, normas, políticas, planes y programas asociados al proceso contable.
12. Hace las veces de secretario dentro del Comité Coordinador de Control Interno, dentro de la Institución.

13. Asesora y Acompaña a las diferentes áreas de la Entidad, para el diseño, documentación e implementación de procesos y sus respectivos puntos de control.

14. Verifica el cumplimiento de metas y objetivos propuestos en los respectivos procesos de cada unidad o área.

15. Asesora y acompaña a las diferentes áreas de la entidad, a fin de que se levante el respectivo mapa de riesgos.

16. Adelanta el respectivo seguimiento a la gestión organizacional, teniendo en cuenta el cumplimiento de metas trazado en el Plan Operativo Anual.

17. Verifica y hace seguimiento al cumplimiento de presentación de los diferentes informes que debe presentar la Institución a las entidades de control.

18. Sirve de apoyo a la alta dirección, para la adopción de nuevos modelos o normatividad relacionada con el Control Interno.

IV. CONOCIMIENTOS BÁSICOS O ESENCIALES

- Constitución Política de Colombia
- Ley 87 de 1993.
- Resolución 048 de 2004.
- Decreto 2145 de 1999.
- Ley 489 de 1998.

- Ley 909 de 2004.
- Ley 734 de 2002.
- Decreto 2539 de 2000.
- Decreto 1599 de 2005. (MECI-1000-2005)
- Plan Operativo Anual de la Entidad.

V. REQUISITOS DE ESTUDIO O EXPERIENCIA

A. EDUCACION: Título Profesional en Economía, Ingeniería Industrial, Contaduría, Administración de Empresas, Derecho.
B. FORMACIÓN: Titulo de Formación avanzada en Administración o Gerencia Pública, Gerencia en Salud, Auditoria Interna, Revisoría Fiscal o áreas administrativas o financieras afines.

C. EXPERIENCIA: Tres (3) años de experiencia Profesional en cargos Directivos o de Asesoría.

IDENTIFICACIÓN

NIVEL:	PROFESIONAL
DENOMINACIÓN DEL EMPLEO:	PROFESIONAL ESPECIALIZADO
CODIGO:	222
GRADO:	7
NUMERO DE CARGOS:	1
DEPENDENCIA:	AREA RECURSOS FISICOS
CARGO DEL JEFE INMEDIATO:	SUBGERENTE ADMINISTRATIVO Y FINANCIERO

I. PROPÒSITO PRINCIPAL

El Hospital Universitario Departamental de Nariño, Empresa Social del Estado, dirigirá sus esfuerzos al mejoramiento continuo y se convertirá en una Institución Centrada en el Usuario. Para alcanzar tales fines implementará un Modelo de Gestión Integral por Calidad.

Será función esencial de los Coordinadores de los Grupos de Trabajo, desplegar el Modelo, las políticas, los objetivos, de la Alta Dirección, a todos los niveles de

su grupo de trabajo, traducirlos a planes operativos, aplicando sistemáticamente el Ciclo PHVA.

II. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Participar activamente en el Proceso de Direccionamiento Estratégico de la Organización.

2. Identificar de manera documentada, a los clientes y proveedores Internos y Externos.

3. Elaborar y documentar el proceso que identifique las necesidades y expectativas de sus clientes, así como el proceso para responder a dichas necesidades.

4. Elaborar y documentar el proceso sistemático para definir y replantear los grandes propósitos institucionales de acuerdo a los cambios del entorno.

5. Participar activamente en la formulación del plan estratégico de la Institución.

6. Elaboración en base a políticas y directrices del Plan Operativo Anual de su Grupo. Dicho Plan debe poseer los objetivos y metas en términos medibles, en concordancia con los objetivos estratégicos de la Institución.

7. Elaborar el cuadro de indicadores claves, que permitan monitorizar las metas y objetivos propuestos.
8. Presentar mensualmente el informe de su gestión, que incluya cuantitativamente, la Gestión realizada.

9. Análisis, evaluación y estandarización del proceso de apoyo de atención al usuario.

10. Construcción de indicadores, evaluación y ciclo de mejora del proceso de apoyo de Atención al Usuario.

11. Dentro del concepto de gerencia ínter funcional, participar activamente, en el proceso asistencial del sistema único de acreditación y los demás estándares de apoyo del sistema de acreditación.

12. Participar, de acuerdo a su competencia, en el Diseño, documentación, prueba, validación, ajuste, socialización e implementación de todos los Procesos de los Estándares de Acreditación de Atención al Cliente Asistencial que se desarrollan en la Sección o en los cuales ésta interviene.

13. Participar, de acuerdo a su competencia, en las actividades de los Procesos de los Estándares de Acreditación de Direccionamiento que se desarrollan en la Sección, o en los cuales ésta interviene.

14. Participar, de acuerdo a su competencia, en el diseño, documentación, prueba, validación, ajuste, socialización e implementación de todos los Procesos de los Estándares de Acreditación de Gerencia que se desarrollan en la Sección o en los cuales ésta interviene

15. Participar, de acuerdo a su competencia, en la elaboración, implementación y evaluación del Plan de Acción para la Monitorización y Mejoramiento de la Calidad.

16. Participar, de acuerdo a su competencia, en el diseño, documentación, prueba, validación, ajuste, socialización e implementación de todos los Procesos de los Estándares de Acreditación de Gerencia de Recursos Humanos que se desarrollan en la Sección o en los cuales ésta interviene

17. Evaluar el desempeño de todo el Personal adscrito a la Sección en coordinación con la Sección de Recursos Humanos.

18. Apoyar los procesos y programas de la Salud Ocupacional y Seguridad Industrial institucional que le competan.

19. Apoyar la Evaluación de la satisfacción de los empleados adscritos a la Sección que adelante la Oficina de Recursos Humanos.

20. Velar porque los resultados de las actividades del mejoramiento de la calidad en la Sección sean comunicados.
21. Liderar la aplicación de los procesos que garanticen el manejo seguro del espacio físico, equipos e insumos, tanto para los trabajadores como para los clientes durante el proceso de atención en la Sección de Suministros.

22. Conocer y hacer cumplir las actividades que le competa de acuerdo con el plan de emergencias y desastres; y de prevención y respuesta a incendios.

23. Liderar el diseño, documentación, prueba, validación, ajustes, socialización e implementación del plan para mejorar la calidad de los procesos de la gerencia del ambiente físico.

24. Adelantar las acciones que le competan en el diseño e implementación de actividades de mejoramiento dentro de las prioridades seleccionadas en el respectivo plan.

25. Velar porque los resultados de las actividades del mejoramiento de la calidad del Ambiente Físico en la Institución sean comunicados.

26. Participar, de acuerdo a su competencia, en el Diseño, documentación, prueba, validación, ajuste, socialización e implementación de todos los Procesos de los Estándares de Acreditación de Gerencia de la Información que se desarrollan en la Sección o en los cuales ésta interviene.

27. Identificar las necesidades de información al interior de la Sección, en especial de aquellas necesidades directamente relacionadas con el proceso de atención a un cliente.

28. Participar en las investigaciones que se realicen cuando el análisis periódico de la información detecte variaciones no esperadas en el desempeño de los procesos o equipos, y en la definición de acciones preventivas y correctivas.

29. Conocer y hacer cumplir con lo estipulado en el Reglamento Interno.

30. Elaborar el Plan Anual de Vacaciones y determinar las necesidades adicionales de Personal en la Sección

31. Asistir a cursos, talleres y reuniones programados por la Sección o por la Institución

32. Elaborar y presentar en forma oportuna a quien corresponda los Informes sobre las actividades desarrolladas, los problemas observados en el desarrollo de las mismas y las correspondientes propuestas de solución

33. Planificar, coordinar, dirigir, supervisar y hacer seguimiento al desarrollo integral de los Procesos y las actividades relacionadas con la prestación de los servicios administrativos de la Sección, que garantice el cabal cumplimiento de las respectivas metas previamente establecidas

34. Liderar la planificación, coordinación y supervisión de todas las actividades relacionadas con los Planes de Mejoramiento de los Procesos que se lleven a cabo en la Sección

35. Elaborar Proyectos orientados al mejoramiento de la calidad en la prestación de los servicios administrativos de la Sección

36. Revisar y firmar el inventario de Activos Fijos de la Institución

37. Cumplir con las actividades que le competen dentro del Plan de Emergencias Hospitalarios

38. Supervisar permanentemente el desempeño del Personal a su cargo

39. Apoyar a la Jefatura de Recursos Humanos en la programación y coordinación del proceso de inducción del Personal que se vincula a la Sección

40. Participar en la Planificación y el Desarrollo del Plan de Capacitación del Personal a su cargo en la Sección, en lo que respecta a formación, adiestramiento y educación continuada

41. Participar y apoyar el desarrollo de las actividades que sobre Salud Ocupacional se lleven a cabo en la Sección.

42. Revisar y Hacer los ajustes que corresponda al Pedido de Materiales y Suministros, de la Sección

43. Velar por el correcto uso de los equipos y elementos que estén bajo su cargo.

44. Garantizar y Mantener la adecuada funcionalidad y comunicación de la Dependencia a su cargo con la Gerencia, las Subgerencias Administrativa y de Prestación de Servicios, las oficinas del nivel Asesor, y las demás secciones de apoyo administrativo, logístico y asistencial, con el fin de: conseguir complementariedad en las conceptualizaciones; mantener los recursos humanos, físicos, financieros y de información que requiera su dependencia; y operativizar las decisiones tomadas.

45. Liderar la elaboración del plan anual de compras; coordinar su consecución; y controlar la recepción.

46. Identificar y programar las necesidades requeridas por la Sección a su cargo, y controlar el gasto y la utilización de las mismas.

47. Elaborar el Plan Operativo Anual del Área bajo su cargo ; definir los Indicadores de Gestión y Resultado de acuerdo a lo previsto en el Plan Operativo Anual; coordinar y ejecutar el desarrollo del Plan Operativo; recolectar información para alimentar los Indicadores de Gestión y Resultado, Analizar su comportamiento (causas y efectos), e Identificar y Aplicar Acciones Correctivas correspondientes; y Mantener informado a su Superior del cumplimiento del Plan Operativo con el fin de lograr su adecuado cumplimiento.

48. Garantizar la adecuada integración de la Misión, Visión, Objetivos y Estrategias Corporativas de la Empresa con la Misión, Visión, Valores, Metas y Acciones propias de la Dependencia a su cargo; promover la adecuada aplicación de las políticas corporativas y del plan de Desarrollo Institucional, informando las decisiones de los Directivos de la Entidad en la Dependencia a su cargo; y

desarrollar estos elementos de Planeación Estratégica mediante su adopción en el Plan Operativo Anual.

49. Liderar la normalización y estandarización de los procesos técnicos y administrativos de la Dependencia a su cargo, mediante la actualización del Manual de Procedimientos y Funciones; Garantizar la adecuada coordinación funcional de procesos, productos y clientes propios de la Dependencia a su cargo, con todas las secciones administrativas y asistenciales de la Institución; Definir Indicadores de Gestión y Resultado de los Procesos que se desarrollan en el Área;

50. Planear, organizar, desarrollar, evaluar y controlar todas las actividades relacionadas con el diseño, elaboración, gestión, ejecución y control de los proyectos del Área aprobados por la Dirección del Hospital.

51. Velar por la debida conservación y el mantenimiento de todos los bienes que posee la Dependencia a su cargo, para el normal desempeño de sus objetivos.

52. Asistir a los diferentes Comités en que tenga asiento la dependencia a su cargo.

53. Desempeñar las demás funciones que se deriven de la organización de procesos internos de la Institución.

III. CONTRIBUCIONES INDIVIDUALES

1. La realización de las actividades responde a prestación de servicios con criterios de calidad humana y tecnológica.

2. El cumplimiento de las tareas se fortalece y se enfoca en exceder las expectativas de los usuarios que hacen uso de los servicios.

3. Contribuir en el adecuado manejo de los insumos y/o equipos de uso diario en el desarrollo de sus funciones.

4. Reconocer las acciones pertinentes y actuar de acuerdo a ellas dentro del Plan de Emergencias Hospitalarias.

IV. CONOCIMIENTOS BASICOS O ESENCIALES

• Ley 100

• Decreto 1011 Sistema Obligatorio de Garantía de la Calidad

• Normas ISO – 9001 / 2000

• Plan de Emergencias Hospitalario

• Estatuto de Contratación

V. REQUISITOS DE ESTUDIO Y EXPERIENCIA

A. EDUCACION: Título Profesional en Economía, Administración, Ingeniería Industrial, Contaduría.

B. FORMACIÓN: Título de Formación Avanzada o Postgrado en áreas de la Salud o Administrativas.

C. EXPERIENCIA: Dos (2) años de experiencia Profesional, uno de los cuales requiere experiencia específica, la cual se entiende como la adquirida en empleos con funciones similares a las del cargo en el Sistema General de Seguridad Social en Salud.

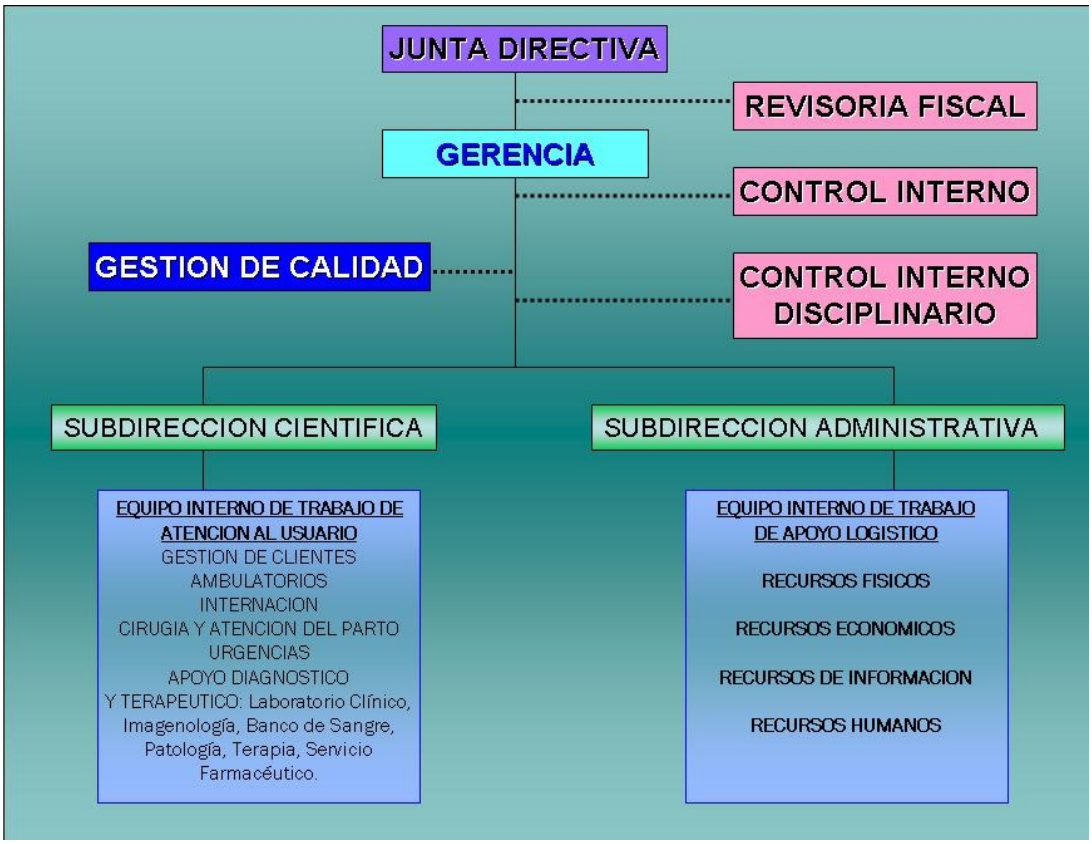
3.1.3. Hospital Civil de Ipiales E.S.E

- **Misión.** Prestar servicios de salud con altos niveles de calidad humana, técnica y científica percibida por el usuario, contribuyendo al mejoramiento de las condiciones de vida de la población.

- **Visión.** Ser una Institución líder en la prestación de servicios de salud con calidad, garantizando al usuario seguridad durante el proceso de atención, mediante el fortalecimiento integral del talento humano, mejoramiento de la infraestructura y renovación tecnológica.

- **Organigrama Hospital Civil de Ipiales E.S.E**

Figura 2: Organigrama Hospital Civil de Ipiales E.S.E.



http://www.hospitalcivil.com/index.php?op=1&sec=4

- **Manual de Funciones del Hospital Civil de Ipiales (Comité de Contratación).** Se transcribió el manual de funciones del comité de contratación extraído del manual de funciones general del Hospital Civil de Ipiales.

IDENTIFICACION

NIVEL:	DIRECTIVO
DENOMINACIÓN DEL EMPLEO:	GERENTE DE EMPRESA SOCIAL DEL ESTADO
CODIGO:	085
GRADO:	02
NUMERO DE CARGOS:	1

DEPENDENCIA: GERENCIA
CARGO DEL JEFE INMEDIATO: JUNTA DIRECTIVA

I. PROPÓSITO PRINCIPAL

Ejercer funciones de dirección, planeación, evaluación y control en la administración y gestión de la entidad.

II. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Dirigir la Empresa, manteniendo la unidad de procedimientos e intereses en torno a la misión y objetivos de la misma.

2. Realizar la gestión necesaria para lograr el desarrollo de la empresa, de acuerdo con los planes y programas establecidos, teniendo en cuenta los perfiles epidemiológicos del área de influencia, las características del entorno y las condiciones internas de la Empresa.

3. Articular el trabajo que realizan los diferentes niveles de la organización, dentro de una concepción participativa de la gestión.

4. Ser nominador y ordenador del gasto, de acuerdo con las facultades concedidas por la Ley y los reglamentos.

5. Velar por el cumplimiento de las leyes y reglamentos que rigen la Empresa.

6. Rendir los informes que le sean solicitados por la Junta directiva y demás Autoridades competentes.

7. Desarrollar planes, programas y proyectos de salud conforme a la realidad socio-económica y cultural de la región.

8. Planear, organizar y evaluar las actividades de la entidad y velar por la aplicación de las normas y reglamentos que regulan el Sistema General de Seguridad Social en Salud.

9. Promover la adaptación, adopción de las normas técnicas y modelos orientados a mejorar la calidad y eficiencia en la prestación de los servicios de salud y velar por la validez científica y técnica de los procedimientos utilizados en el diagnóstico y tratamiento.

10. Velar por la utilización eficiente de los recursos humanos, técnicos y financieros de la entidad y por el cumplimiento de las metas y programas aprobados por la Junta Directiva.

11. Presentar para la aprobación de la Junta Directiva el plan trienal, los programas anuales de desarrollo de la entidad y el presupuesto respectivo, de acuerdo con la Ley Orgánica de Presupuesto y normas reglamentarias.

12. Adaptar la entidad a las nuevas condiciones empresariales establecidas en el marco del sistema General de Seguridad Social en Salud, garantizando tanto la eficiencia social como económica de la entidad, así como la competitividad de la institución.

13. Organizar el sistema contable y de costos de los servicios y propender por la eficiente utilización del recurso financiero.

14. Garantizar el establecimiento del sistema de acreditación hospitalaria, de auditoria en salud y control interno que propicien la garantía de la calidad en la prestación del servicio.

15. Liderar la organización de sistemas de referencia y contrarreferencia de pacientes de conformidad con las disposiciones de la Dirección Seccional de salud y las características de las empresas promotoras de salud, y contribuir a la organización de las redes o nodos de servicios en la región.

16. Diseñar y poner en marcha un sistema de información en salud, según las normas técnicas que expida el Ministerio de la Protección Social y adoptar los procedimientos para la programación, ejecución, evaluación, control y seguimiento físico y financiero de los programas.

17. Fomentar el trabajo en equipo, con un enfoque interdisciplinario y promover la coordinación intra e intersectorial.

18. Desarrollar objetivos, estrategias y actividades conducentes a mejorar las condiciones laborales, el clima organizacional, la salud ocupacional y el nivel de capacitación y entrenamiento, y en especial ejecutar un proceso de educación continua para todos los funcionarios de la entidad.

19. Presentar a la Junta Directiva el proyecto de planta de personal y las reformas necesarias para su adecuado funcionamiento y someterlos a la aprobación de la autoridad competente.

20. Nombrar y remover los funcionarios bajo su dependencia de acuerdo con las normas de administración de personal que rigen para las diferentes categorías de empleos en el sistema General de Seguridad Social en Salud.

21. Diseñar modelos y metodologías para estimular y garantizar la participación ciudadana y propender por la eficiencia de las actividades extramurales en las acciones tendientes a lograr metas de salud y el mejoramiento de la calidad de vida de la población.

22. Diseñar mecanismos de fácil acceso a la comunidad, que permitan evaluar la satisfacción de los usuarios, atender las quejas y sugerencias y diseñar en consecuencia, políticas y correctivos orientados al mejoramiento continuo de los servicios.

23. Representar legalmente a la entidad judicial y extrajudicial y ser ordenador del gasto.

24. Firmar las convenciones colectivas con los trabajadores oficiales de acuerdo con la disponibilidad presupuestal.

25. Contratar con las Entidades Promotoras de Salud públicas o privadas la realización de las actividades del Plan Obligatorio de Salud que esté en capacidad de ofrecer.

26. Propiciar y desarrollar investigaciones científicas y tecnológicas con el fin de establecer las causas y soluciones a los problemas de salud en su área de influencia.

27. Adelantar actividades de transferencia tecnológica y promover la realización de pasantías con el fin de ampliar los conocimientos científicos y tecnológicos de los funcionarios de la Empresa.

28. Participar y contribuir al desarrollo del sistema de la red de urgencias en su área de influencia.

29. Promocionar el concepto de gestión de calidad y acreditación que implique contar con estrategias coherentes de desarrollo organizacional.

30. Presentar los proyectos de Acuerdo o Resoluciones a través de los cuales se decidan situaciones en la empresa que deben ser adoptadas o aprobadas respectivamente por la Junta Directiva.

31. Celebrar o suscribir los contratos de la empresa.

32. Coordinar el diseño de portafolios de servicios de acuerdo a la demanda y necesidades de la comunidad.

33. Facilitar y comprometerse con el proceso de Direccionamiento estratégico de la organización.

34. Desarrollar junto con la Junta Directiva y demás personal de la Empresa el análisis estratégico, donde se incluya la lectura del entorno, la voz del cliente interno, las necesidades del paciente y su familia y ejercicios de referenciación competitiva.

35. Construir a partir del análisis estratégico el plan de direccionamiento estratégico de la Empresa.

36. Es responsable de la difusión y seguimiento del Direccionamiento Estratégico de la Empresa.

37. Establecer junto con el personal a su cargo los parámetros de monitorización de la ejecución de los planes de manera tal que se garantice la viabilidad financiera de la organización.

38. Definir junto con el personal a su cargo procesos para evaluar integralmente la gestión en salud para los clientes, con base en procesos de auditoria de la calidad en la organización, haciendo seguimiento a indicadores trazadores.

39. Establecer parámetros de orientación al personal de manera alineada con el Direccionamiento Estratégico de la Organización.

40. Establecer de manera compartida con los trabajadores, usuarios y proveedores planes para mejorar la calidad de los procesos de direccionamiento estratégico.

41. Las demás que establezca la Ley, los Reglamentos y la Junta Directiva de la Empresa.

III. CONTRIBUCIONES INDIVIDUALES (CRITERIOS DE DESEMPEÑO)

1. La organización administrativa y financiera de la entidad cumple con las nuevas condiciones empresariales establecidas en el marco del Sistema General de Seguridad Social en Salud, en cuanto a racionalidad, eficiencia en el servicio público y competitividad de la institución.

2. El sistema contable y de costos de los servicios se encuentra documentado y refleja la realidad financiera de la prestación de los servicios.

3. Los indicadores de calidad en la prestación del servicio reflejan mejoramiento continuo con base en la aplicación del sistema de acreditación hospitalaria, de auditoria en salud y control interno.
4. Se desarrolla un proceso de direccionamiento estratégico participativo, orientado a vincular a la organización con el entorno, a proveerle una noción de largo plazo y a buscar la solidaridad de la persona para el logro de objetivos comunes.

5. Se desarrollan procesos de despliegue del direccionamiento estratégico de manera tal que se genere interrelación entre el plan estratégico y el desempeño operativo de los procesos, garantizando que cada trabajador tenga los recursos para la ejecución de su tarea y asuma la responsabilidad por los resultados del mismo.

6. Controla y evalúa periódicamente los indicadores estratégicos, para apalancar la consecución del sueño de futuro de la organización.

7. Realiza un proceso de revisión por la Dirección al Sistema de Gestión de Calidad, para contribuir a su mejoramiento continuo.

8. Realiza reuniones periódicas con el personal con el propósito de desplegar resultados obtenidos y generar recomendaciones orientadas a apalancar la consecución del sueño de futuro y los objetivos estratégicos de la empresa.

III. CONOCIMIENTOS BÁSICOS O ESENCIALES

- Constitución Nacional.
- Normas legales vigentes para el sector salud.
- Leyes 100 de 1993 y 872 del 2004.
- Implementación del Sistema de Gestión de Calidad en el sector Público.
- Decreto 4110 de 2004.
- NTC ISO 9001, capítulos 4 y 5.

IV. REQUISITOS DE ESTUDIO Y EXPERIENCIA

Estudios: Título profesional en áreas de la salud, económicas, administrativas o jurídicas y Título de postrado en salud pública, administración o gerencia hospitalaria, administración en salud u otro en administración en salud.

Experiencia: Experiencia profesional de tres (3) años en el sector salud.

IDENTIFICACION

NIVEL:	DIRECTIVO
DENOMINACIÓN DEL EMPLEO:	SUBDIRECTOR ADMINISTRATIVO
CODIGO:	068
GRADO:	1
NUMERO DE CARGOS:	1
DEPENDENCIA:	APOYO LOGÍSTICO
CARGO DEL JEFE INMEDIATO:	GERENTE

I. PROPÓSITO PRINCIPAL

Dirigir, planear, coordinar y controlar los procesos operativos, administrativos y financieros, de acuerdo con las áreas estructuradas en el organigrama institucional. Procurar la racionalización y adecuada administración de los recursos institucionales, con el fin de garantizar la adecuada prestación de los servicios de salud a la comunidad que pertenece el área de influencia del Hospital Civil de Ipiales, E.S.E.

II. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Realizar periódicamente junto con la Subdirección Científica y Gerencia un análisis estratégico del entorno interno y externo de la entidad.

2. Conformar junto con la Gerencia y la Subdirección Científica el equipo encargado de la elaboración del plan estratégico desarrollo de la entidad.

3. Elaborar periódica y sistemáticamente un proceso de monitorización, seguimiento y mejoramiento de la calidad de todas y cada una de las áreas de su responsabilidad.

4. Dirigir, programar, coordinar y controlar los procesos administrativos y financieros del Hospital Civil de Ipiales, E.S.E.

5. Asesorar a la Gerencia en la toma de decisiones de carácter administrativo y/o financiero.

6. Planear, dirigir, coordinar y controlar el funcionamiento de los aspectos relativos a los procesos de Gestión de Recursos Económicos, Gestión de Recursos Humanos, Gestión de Recursos Físicos y Gestión de Recursos de Información.

7. Dirigir, organizar y controlar las actividades del personal que interviene técnica, operativa y administrativamente en la ejecución de las labores que adelanta el Hospital Civil de Ipiales a fin de que se cumplan los objetivos propuestos.

8. Velar por una adecuada aplicación de las políticas de selección, desarrollo y bienestar del recurso humano del hospital.

9. Establecer y mantener mecanismos de coordinación intersectorial con entidades que operan dentro del área de influencia del hospital, a fin de lograr el apoyo logístico y asistencial que facilite la prestación de los servicios, suministrados por los diferentes procesos a través de los indicadores de gestión.

10. Analizar la información estadística suministrada por los diferentes procesos a través de los indicadores de gestión para una eficaz toma de decisiones administrativas.

11. Supervisar la oportuna prestación de los servicios generales, de correspondencia y transporte en los diferentes procesos institucionales.

12. Coordinar con la Subdirección Científica la realización de actividades dirigidas a la identificación de problemas internos institucionales y la formulación de estrategias de solución.

13. Controlar la ejecución de los procesos internos, inspeccionar su calidad con criterios técnicos y a través de la revisión permanente de no conformidades e informes de auditoría para trazar los correctivos pertinentes si es necesario hacerlo.

14. Evaluar los mecanismos de control interno y sugerir cambios que garanticen la calidad de los procesos.

15. Coordinar la actualización periódica de los Manuales de Funciones, de Procesos Administrativos y Operativos, de Archivo y Correspondencia, de Control Interno y demás documentos de organización interna, de acuerdo a las nuevas disposiciones y necesidades de la Institución.

16. Presidir el Comité de Compras de la Institución, garantizando transparencia y un adecuado manejo y elección de los proveedores de la entidad.

17. Vigilar y velar por el cumplimiento de las leyes, estatutos, reglamentos, acuerdos de la Junta Directiva y demás disposiciones aplicables a la Entidad.

18. Controlar y velar por el pronto pago de las obligaciones adquiridas por la Entidad.
19. Coordinar la elaboración del Proyecto Anual de Presupuesto para ser discutido y evaluado con la Gerencia.

20. Analizar periódicamente en conjunto con la Subdirección científica y la unidad financiera los estudios de costos de la institución, con el fin de plantear medidas correctivas respecto a la redistribución de ingresos o disminución de gastos.

21. Formular propuestas para la generación de recursos económicos adicionales a través de nuevos servicios y/o alternativas de inversiones financieras que contribuyan a la solidez institucional.

22. Coordinar la realización de inventarios físicos que se efectúen en la Institución.

23. Promulgar y aplicar mecanismos de control que garanticen el correcto manejo y utilización de los recursos físicos de la Entidad.

24. Ordenar los gastos de caja menor de acuerdo a la delegación efectuada por la Gerencia.

25. Reemplazar a la Gerencia en sus inasistencias temporales, y/o cuando así se delegue.

26. Representar a la Gerencia en las actividades, eventos o reuniones que así se deleguen.

27. Presentar a la Gerencia el informe de cada asistencia a seminarios, reuniones y eventos en general a los que asista como invitado, participante o delegado por parte del Hospital Civil de Ipiales, E.S.E.

28. Coordinar la elaboración y presentación oportuna de los informes requeridos por la Gerencia, la Junta Directiva, la Superintendencia de Industria y Comercio y demás unidades administrativas.

29. Controlar y hacer cumplir la relación de envíos de las obligaciones con la Contraloría General de la República, DIAN y Bancos, en las fechas estipuladas.

30. Conocer, desplegar y aplicar el modelo de gestión adoptado por la Institución.

31. Cumplir y hacer cumplir los deberes y derechos de los usuarios incorporados dentro del Direccionamiento institucional.

32. Participar en la elaboración y socialización del Direccionamiento Estratégico Institucional.

33. Participar en la definición de objetivos y metas acordes a la política institucional.

34. Cumplir y velar por el cumplimiento del código único disciplinario (ley 734 del 2002).

35. Elaborar periódica y sistemáticamente un proceso de monitorización, seguimiento y mejoramiento de la calidad de todas y cada uno de los servicios de su responsabilidad.

36. Actualizar periódicamente la información necesaria de su área, la cual permite la elaboración de Plan Estratégico Institucional.

37. Divulgar y alinear al personal a su cargo, acerca de procesos, estandarización, mejoramiento continuo, entre otros aspectos, lo cual permita mejorar la productividad de su área de trabajo.

38. Elaborar y actualizar periódica y sistemáticamente los manuales de procesos, registros y demás documentos soportes del sistema de gestión de calidad de cada una de las áreas donde se es responsable.

III. CONTRIBUCIONES INDIVIDUALES (CRITERIOS DE DESEMPEÑO)

1. Los servicios administrativos se ajustan a la planeación de la entidad, se desarrolla de manera coordinada y controlada con las demás dependencias de la entidad.

2. La mejora en los servicios administrativos se caracteriza por la actualización permanente de procesos y procedimientos, y por la búsqueda constante de soluciones a problemas concretos.

3. Las normas y procedimientos se aplican de conformidad a los modelos establecidos y buscan la optimización de las actividades disminuyendo retrasos y pérdidas de tiempo y recursos.

4. La coordinación a todo nivel se promueve como mecanismo para potenciar los resultados positivos que difícilmente se lograrían sin trabajo en equipo.

5. Los manuales de normas y procedimientos administrativos se difunden, actualizan y mejoran cada vez que se requiere, en concurrencia con las directrices que se definen a nivel superior.
6. Los recursos se gestionan oportunamente y permiten ser aplicados de forma planificada para la buena marcha de la entidad.

7. Los estudios de satisfacción del cliente se desarrollan siguiendo parámetros de búsqueda de excelencia en el servicio prestado, se basan en metodologías universalmente aplicadas y con respaldo técnico.

8. Los avances y desarrollos en la implementación del sistema de gestión de calidad reflejan el impacto en los procesos y la mejora continua de los mismos.

IV. CONOCIMIENTOS BÁSICOS O ESENCIALES

- Constitución Nacional.
- Normas vigentes para el sector salud.
- Programas señalados por el Ministerio de la Protección Social.
- Mecanismos de participación comunitaria en el sector salud.
- Metodologías de investigación y diseño de planes, programas y proyectos.
- Estructura administrativa de la entidad.
- Manual de funciones y competencias laborales mínimas de la entidad.
- Manuales de procesos y procedimientos administrativos de la entidad y del sector salud.

V. REQUISITOS DE ESTUDIO Y EXPERIENCIA

Estudios: Título profesional en áreas administrativas, económicas o financieras, derecho, ingeniería industrial y Título de postgrado en administración, alta gerencia, finanzas, administración de la salud, gerencia y auditoría, o estudios afines a su área de desempeño.

Experiencia: Experiencia relacionada con las funciones del cargo de dos (2) años.

IDENTIFICACION

NIVEL:	DIRECTIVO
DENOMINACIÓN DEL EMPLEO:	SUBDIRECTOR CIENTÍFICO
CODIGO:	072
GRADO:	1
NUMERO DE CARGOS:	1

DEPENDENCIA: ATENCIÓN AL USUARIO
CARGO DEL JEFE INMEDIATO: GERENTE

I. PROPÓSITO PRINCIPAL

Liderar los procesos administrativos y asistenciales y gestionar los planes y proyectos de las diferentes secciones de Urgencias, Servicios Ambulatorios e Internación, Apoyo Diagnóstico y Soporte Terapéutico, Quirófanos y Sala de Partos.

II. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Cumplir y hacer cumplir los deberes y derechos de los usuarios incorporados dentro del plan de direccionamiento institucional.

2. Conocer, desplegar y aplicar el modelo de gestión adoptado por la Institución.

3. Saludar al usuario y su familia, presentarse y explicarles cuál va ser su participación durante el proceso de atención.

4. Participar en la elaboración y socialización del Direccionamiento estratégico institucional.

5. Participar en la definición de objetivos y metas de las secciones asistenciales acordes a las políticas institucionales.

6. Participar en la elaboración y difusión del portafolio de servicios Institucional.

7. Evaluar el desempeño del personal a su cargo.

8. Realizar y coordinar las actividades de inducción y capacitación al personal del área.

9. Cumplir y velar por el cumplimiento del código único disciplinario (Ley 734 del 2002).

10. Liderar los procesos específicos del área como de Auditoría, Contratación, Quejas y Reclamos, monitoriza los resultados de cada sección y coordinar la elaboración e implementación del plan de mejora según los resultados de la evaluación.

11. Presentar la información gerencial requerida.

12. Liderar los diferentes comités establecidos en la institución afines al área.

13. Participar en los diferentes comités técnicos administrativos propios del cargo.

14. Liderar los planes, proyectos, programas de salud y procesos implementados en el área.

15. Liderar y desarrollar eventos y reuniones científicas, investigativas.

16. Coordinar la asignación y utilización de los recursos humanos y logísticos.

17. Realizar las actividades específicas teniendo en cuenta su participación en los procesos implementados en cada sección.

18. Lidera los planes de contingencia y emergencia del área asistencial.

19. Liderar procesos orientados a definir participativamente los protocolos de atención clínica para las patologías que corresponde el perfil epidemiológico y monitorizar su correcta aplicación.

20. Levantar, ejecutar y monitorizar los procesos críticos de su área.

21. Y todas las demás funciones que se le asignen de acuerdo a la naturaleza del cargo.

III. CONTRIBUCIONES INDIVIDUALES (CRITERIOS DE DESEMPEÑO)

1. Los servicios de salud se monitorean continuamente y se detectan posibles falencias a fin de ser corregidas en pro de prestar servicios médicos de óptima calidad y se evalúan periódicamente el impacto de las acciones correctivas tomadas.

2. Los resultados del sistema de auditoría médica, permiten planear y controlar el mejoramiento en la prestación de los servicios de salud de la entidad.

3. Los procedimientos médicos se revisan continuamente para mejorar su eficiencia y eficacia en el tratamiento integral de la enfermedad y el paciente, se siguen parámetros científicos para la validación de las mejoras o variaciones de las técnicas y procedimientos.
4. El sistema de referencia y contrareferencia sigue los parámetros establecidos por el Ministerio de la Protección Social y los registros permiten la verificación del funcionamiento adecuado.

5. La vigilancia epidemiológica se desarrolla en el marco de los procesos establecidos para esta acción y es una actividad de tipo permanente.
6. Se evalúan las acciones y resultados de las actividades producto de la coordinación intra e intersectorial.

7. Se lidera procesos administrativos y asistenciales y gestionan los planes y proyectos de las diferentes secciones de Urgencias, Servicios Ambulatorios e Internación, apoyo diagnóstico y Soporte Terapéutico, Cirugía y Sala de Partos.

8. Se propende por hacer cumplir los deberes y derechos de los usuarios incorporados dentro del plan de direccionamiento institucional.

IV. CONOCIMIENTOS BÁSICOS O ESENCIALES

- Constitución Nacional.
- Normas vigentes para el sector salud.
- Programas señalados por el Ministerio de la Protección Social.
- Mecanismos de participación comunitaria en el sector salud.
- Metodologías de investigación y diseño de planes, programas y proyectos.
- Sistemas de referencia y contrarreferencia.
- Ley 100 de 1993 y sus Decretos Reglamentarios.

V. REQUISITOS DE ESTUDIO Y EXPERIENCIA

Estudios: Título profesional en Medicina y Título de postgrado en Gerencia o Administración de la Salud o afines.

Experiencia: Experiencia profesional de dos (2) años.

IDENTIFICACION

NIVEL:	PROFESIONAL
DENOMINACIÓN DEL EMPLEO:	PROFESIONAL UNIVERSITARIO
CODIGO:	219
GRADO:	5
NUMERO DE CARGOS:	1
DEPENDENCIA:	APOYO LOGÍSTICO
CARGO DEL JEFE INMEDIATO:	SUBDIRECTOR ADMINISTRATIVO

I. PROPÓSITO PRINCIPAL

Ejecutar labores de asesoría a nivel profesional en aspectos jurídicos en una institución del sistema de salud.

II. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Asesorar al Gerente, Subdirector Científico, Subdirector Administrativo y demás directivos en los asuntos jurídicos relacionados con la entidad y emitir los conceptos que se requieran por las diferentes dependencias.

2. Conceptuar sobre los asuntos jurídicos relacionados con el Hospital, cuya competencia no haya sido asignada a otras entidades o dependencias.

3. Contribuir al estudio de temas que, según su naturaleza, hayan sido proyectados y debatidos en otras dependencias o entidades, y respecto de los cuales haya de fijarse la posición jurídica del Hospital.

4. Preparar y revisar los proyectos de acuerdos de la Junta Directiva, en asunto de naturaleza jurídica, así como los demás actos de esa naturaleza que daban expedirse al interior de la entidad.

5. Representar jurídicamente al Hospital cuando así le sea encomendado por la Gerencia, y mantener a dicha dependencia siempre informada del avance de los negocios.

6. Establecer criterios de interpretación legal de última instancia al interior de la entidad.

7. Recopilar, actualizar y sistematizar las normas legales y reglamentarias que hagan relación con la actividad del Hospital.

8. Preparar y revisar las minutas de contratos, los pliegos de invitaciones o licitaciones según las características de la entidad, los proyectos de resolución y otros actos administrativos que se sometan a su consideración.

9. Rendir los informes periódicos y los demás que sean solicitados por la Gerencia.

10. Asesorar jurídicamente en la definición de los convenios interinstitucionales de cooperación y asesorar en lo concerniente a los convenios que para el efecto se realicen.

11. Conocer, desplegar y aplicar el modelo de gestión adoptado por la entidad.
12. Cumplir y hacer cumplir los deberes y derechos de los usuarios incorporados dentro del Direccionamiento institucional.

13. Participar en la elaboración y socialización del direccionamiento Estratégico institucional.

14. Participar en la definición de los objetivos y metas acordes a la política institucional.

15. Cumplir y velar por el cumplimiento del código único disciplinario (ley 734 del 2002).

16. Elaborar periódica y sistemáticamente un proceso de monitorización, seguimiento y mejoramiento de la calidad de todas y cada uno de los servicios de su responsabilidad.

17. Estudiar, clasificar y valorar los cargos y puestos de trabajo según las normas y procedimientos establecidos.

18. Desarrollar y aplicar los instrumentos técnicos necesarios para la selección y evaluación del personal y tramitar la inscripción de los funcionarios a carrera administrativa.

19. Levantar, estandarizar de manera participativa con otra instancia de la organización, los procesos para identificar y responder a las necesidades identificadas de los clientes internos de la organización.

20. Establecer procesos orientados a la planeación del Recurso Humano, de acuerdo a los cambios que se susciten en el ambiente.

21. Garantizar que el personal de la institución profesional y no profesional cuente con la suficiente calificación y competencia para el trabajo a desarrollar.

22. Adelantar procesos para identificar las necesidades de educación continuada, el cual debe ser planeado de acuerdo a la necesidad del cliente interno.

23. Identificar y mejorar mediante la monitorización permanente los procesos críticos de su equipo funcional.

24. Programar y aplicar de manera coordinada con otras dependencias los mecanismos de evaluación de desempeño del personal vinculado, conforme con

los instrumentos de evaluación adoptados por el Departamento Administrativo de la Función Pública.

25. Formular en conjunto con la comisión de personal y otras áreas los programas de capacitación, desarrollo y bienestar social y laboral de los funcionarios del Hospital.

26. Adelantar estudio de necesidades cualitativas y cuantitativas de Recursos Humanos, para consolidar las características, costos y ubicación de funcionarios, en coordinación con otras áreas de la empresa.

27. Verificar que el Programa de Salud Ocupacional se cumpla debidamente con los responsables de las diferentes áreas.

28. Supervisar y evaluar el correcto manejo de novedades laborales.

29. Notificar oportunamente a la Administradora de Riesgos Laborales, la ocurrencia de accidentes de trabajo o enfermedades profesionales.

30. Revisar la liquidación de nómina, prestaciones sociales, Seguridad Social y parafiscales e igualmente honorarios por servicios personales prestados por contratistas, y elaborar los actos administrativos correspondientes.

31. Coordinar y verificar la aplicación del programa de inducción de personal, así como su vinculación a regímenes de Seguridad Social.

32. Actualizar el Manual de Funciones de acuerdo a las variaciones del Plan de cargos de la empresa.

33. Expedir certificaciones del trabajo del personal vinculado o desvinculado del Hospital.

34. Promover y participar en la ejecución de programas recreativos de los usuarios internos y externos que contribuyan al esparcimiento.

35. Velar por la adecuada utilización de los recursos de su dependencia y presentar informes periódicos de las actividades realizadas.

36. Informar a los niveles correspondientes sobre quejas y reclamos presentados por los usuarios.

37. Los demás que le sean asignados de acuerdo a la naturaleza del cargo.

III. CONTRIBUCIONES INDIVIDUALES (CRITERIOS DE DESEMPEÑO)

1. Las actividades de asistencia y asesoría se fundamentan técnica y legalmente y se documentan para garantizar el registro adecuado.
2. Las consultas, quejas, reclamos y derechos de petición se responden de manera oportuna dentro de los términos legales y se ajustan en derecho.

3. Los procesos y procedimientos administrativos se encuentran documentados y actualizados.

4. Los indicadores de gestión y logro se miden periódicamente y se toman las acciones de mejoramiento para alcanzar o superar las metas trazadas.

5. Los informes se presentan de forma oportuna de acuerdo con los cronogramas trazados y cumpliendo los requisitos previstos.

6. Los proyectos de actos administrativos se presentan con arreglo a las normas vigentes en la materia, se tiene como fundamento las directrices impartidas por la alta dirección de la entidad.

7. Las dependencias y funcionarios de la entidad son informados sobre los cambios en la legislación y jurisprudencia vigente en materia de contratación administrativa y se registran las comunicaciones e informes al respecto.

8. Se presentan informes escritos con los resultados del ejercicio de funciones de representación a la entidad.

IV. CONOCIMIENTOS BÁSICOS O ESENCIALES

- Constitución Nacional.
- Régimen legal vigente para la entidad.
- Régimen de contratación administrativa.
- Jurisprudencia y doctrina.
- Estructura del Estado Colombiano.
- Estructura administrativa de la entidad.
- Manual de funciones y competencias laborales mínimas.
- Manuales de procesos y procedimientos administrativos.

V. REQUISITOS DE ESTUDIO Y EXPERIENCIA

Estudios: Mínimo: Título profesional en Derecho.
Experiencia: Experiencia relacionada con las funciones del cargo de dos (2) años.

3.2. ARCHIVO CORRIENTE

Para llevar a cabo el proceso de auditoría se hará una recopilación de documentos que tendrán que ver directamente con este desarrollo.

3.2.1. Programa de Auditoria. Para la realización del proceso de auditoría al proceso de contratación del Hospital Universitario Departamental de Nariño y del Hospital Civil de Ipiales, se utilizara la metodología COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas), se evaluaran algunos objetivos de control que se encuentran dentro de los dominios del COBIT así:

- **DOMINIO - PLANIFICACION Y ORGANIZACIÓN (PO).** Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos de negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas, los procesos que se realizaran y los objetivos de control que se evaluaran son los siguientes.

  - ✓ **Definición de la Arquitectura de Información (PO2).** Busca organizar de manera adecuada los sistemas de información para su posterior utilización, Los objetivos de control a evaluar serán:

    - o **PO2.3 Esquema de Clasificación de datos:** Los datos que se manejen en los procesos deberán ser consistentes y fiables, por lo que se deberá definir, implementar y mantener protocolos de seguridad con los niveles y controles apropiados y acordes a los procesos que se llevan a cabo en estas entidades, ya que se deberá tener en claro que información es publica, privada, confidencial etc. Se deberá definir implementar y mantener controles de acceso, archivo y cifrado para la correcta manipulación de la información.

    - o **PO2.4 Administración de Integridad:** Las entidades señaladas deberán definir e implementar protocolos de seguridad para el manejo de bases de datos, almacenes de datos, y demás información que llegue a la entidad en gran volumen.

  - ✓ **Definición de la organización y de las relaciones de TI (PO4).** Objetivo: Prestación de servicios de TI

Esto se realiza por medio de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas, Los objetivos de control a evaluar serán:

- **PO4.6 Establecimiento de Roles y Responsabilidades:** Las responsabilidades y roles en los procesos y en los respectivos sistemas de información deberán estar bien documentados y definidos con propiedad y anterioridad para darle a los procesos la mayor transparencia posible, esto con el fin de cumplir con los estatutos y leyes que rigen este tipo de actuaciones en entidades publicas. Además la seguridad en este tipo de sistemas deberá ser compartida por las dependencias involucradas sin desconocer responsabilidades individuales.

- **PO4.8 Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento:** Las entidades señaladas deberán determinar con claridad los riesgos a los que se encuentran expuestos los sistemas de información tanto lógicamente como físicamente, esto con el objetivo de asignar responsabilidades especificas sobre este riesgo, también con el fin de asignar roles en toda la organización cuando el estado es critico, además se deberán establecer y tener claros los protocolos necesarios para enfrentar las crisis establecidas; todo lo anterior con el objetivo de no entorpecer el normal funcionamiento de las entidades mencionadas.

- **PO4.9 Propiedad de Datos y de Sistemas:** Las entidades mencionadas deberán asegurar que tanto los sistemas como los datos cuenten con un propietario asignado, que serán responsables del manejo, mantenimiento y seguridad de estos. Estos propietarios de sistemas y datos serán los encargados de implementar los niveles de seguridad apropiados como son manejo de contraseñas, acceso a equipos y sistemas, copias de seguridad y demás que sean necesarias para el manejo de la información en las entidades mencionadas.

- **PO4.10 Supervisión:** Las entidades mencionadas deberán proporcionar certeza en el cumplimiento de los roles y responsabilidades establecidas, deberán identificar si los involucrados en estos roles y responsabilidades cuentan con la suficiente autoridad y recursos para ejercer las tareas impuestas.

- **PO4.11 Segregación de Funciones:** Las entidades mencionadas deberán asegurarse de asignar adecuadamente los roles dentro de los sistemas y de los procesos, esto con el fin de que se reduzca al mínimo la posibilidad de que un evento mal hecho por un solo individuo perjudique todo el proceso y a la entidad en general, además deberá asegurarse que el personal solo podrá realizar las tareas a las que esta autorizado y que son relevantes solo a su dominio laboral.

- **PO4.13 Personal Clave de TI:** Las entidades mencionadas deberán tener identificado al personal clave así como sus funciones y los procedimientos que llevan a cabo, además deberán evitar el máximo que las responsabilidades y procesos críticos recaigan sobre una sola persona, por el contrario estos procesos y responsabilidades deberán ser distribuidas para una mayor seguridad.

- **PO4.14 Políticas y Procedimientos para Personal Contratado:** Las entidades mencionadas deberán asegurarse que al realizar los procesos de contratación, las entidades o personas con las que lo hagan cumplan y garanticen que llevaran a cabo las políticas de protección de los activos de información de la entidad, ajustándose a sus protocolos y al estricto cumplimiento de estos.

- **PO4.15 Relaciones:** Las entidades mencionadas deberán poseer los canales de comunicación necesarios entre dependencias para el correcto funcionamiento de los procesos, de no poseerlos deberán encargarse de crearlos y mantenerlos, estos canales deberán ser directos y adecuados para todo el personal tanto interno o externo que estén involucrados en dichos procesos.

✓ **Administración de recursos humanos (PO7).** Objetivo: Maximizar las contribuciones del personal a los procesos de TI, satisfaciendo así los requerimientos de negocio, a través de técnicas sólidas para administración de personal. Los objetivos de control a evaluar serán:

- **PO7.2 Competencias del Personal:** Las entidades mencionadas deberán asegurarse de verificar que el personal que se encuentra involucrado en el proceso mencionado posea las habilidades suficientes para el cumplimiento de los roles y responsabilidades asignados, esto se verificara por medio de su educación, experiencia o entrenamiento esto se hará con el fin de salvaguardar la información que se manipula en esta clase de procesos siendo el solo el personal mas idóneo el que la maneje y controle.

- **PO7.4 Entrenamiento del Personal de TI:** Las entidades deberán asegurar que garantizaran a los empleados que se vean envueltos en los procesos mencionados la capacitación y el entrenamiento continuo sobre todos los ítems necesarios y en especial el de seguridad para que estos lleven a cabo un buen proceso.

- **PO7.5 Dependencia Sobre los Individuos:** Las entidades deberán garantizar que el conocimiento crítico que poseen los empleados que se ven involucrados en el proceso será capturado por medio de

documentación, sucesión y respaldos con el fin evitar al mínimo la dependencia sobre cualquier individuo.

- ✓ **Evaluación de riesgos (PO9).** Objetivo: Asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI

  Para ello se logra la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos y los objetivos de control a evaluar serán:

  - o **PO9.1 Marco de Trabajo de Administración de Riesgos:** Las entidades mencionadas deberán establecer un plan de trabajo para la administración de riesgos físicos y lógicos que se lleve a cabo en paralelo con los procesos mencionados.

  - o **PO9.3 Identificación de Eventos:** Las entidades mencionadas deberán identificar por medio de un autoexamen los elementos esenciales a que se encuentran expuestos a cualquier nivel de riesgo, tales como activos físicos y lógicos, y deberán identificar las amenazas, vulnerabilidades, protecciones, consecuencias y las probabilidades de que un evento de este tipo ocurra.

  - o **PO9.4 Evaluación de Riesgos de TI:** Las entidades mencionadas deberán establecer un marco de referencia de evaluación sistemática de riesgos. Este trabajo deberá identificar los riesgos de forma cuantitativa y cualitativa para determinar la probabilidad de impacto y sus derivados.

  - o **PO9.5 Respuesta a los Riesgos:** Las entidades mencionadas deberán desarrollar y mantener un proceso de respuesta a cualquier riesgo de los evaluados para asegurar que los controles que se lleven a cabo en las entidades mitigaran las consecuencias de cualquier evento. Este proceso deberá enfocarse no solo en dar respuesta a un evento después de que suceda sino por el contrario deberá tratar de evitar, reducir y compartir los riesgos que se están evaluando.

  - o **PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos:** Las entidades mencionadas deberán mantener el plan de riesgos descrito y monitorearlo permanentemente, además se deberá contar con todas las aprobaciones presupuestales y de personal para llevarlo a cabo.

- **DOMINIO - ADQUISICION E IMPLEMENTACION (AI).** Para llevar a cabo la estrategia de TI, las soluciones de Ti deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento

realizados a sistemas existentes, los procesos que se realizaran y los objetivos de control que se evaluaran son los siguientes.

- ✓ **Adquisición y mantenimiento del software aplicativo (AI2).** Objetivo: Proporciona funciones automatizadas que soporten efectivamente al negocio.

  Para ello se definen declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros. Los objetivos de control a evaluar serán:

  - o **AI2.3 Control y Posibilidad de Auditar las Aplicaciones:** Las entidades mencionadas deberán implementar los controles necesarios en todas las aplicaciones que se vean involucradas en el proceso mencionado, estos controles deberán lograr que el procesamiento sea exacto, oportuno, autorizable y sobre todo auditable.

  - o **AI2.4 Seguridad y Disponibilidad de las Aplicaciones:** La tolerancia a fallos y riesgos por parte de las entidades debe ser alta, por lo tanto se deben identificar los riesgos tanto de arquitectura de la información, clasificación de datos, por tanto las entidades mencionadas deben garantizar que las aplicaciones utilizadas en el proceso mencionado cuenten con los respectivos planes de contingencia que les permitan gozar de alta seguridad y de disponibilidad permanente.

  - o **AI2.10 Mantenimiento de Software Aplicativo:** Las entidades mencionadas deberán realizar mantenimientos preventivos en los aplicativos que se vean involucrados en el proceso mencionado con el fin de reducir la frecuencia y el impacto de las fallas que se pudieran presentar.

- ✓ **Adquisición y mantenimiento de la infraestructura tecnológica (AI3).** Objetivo: Proporcionar las plataformas apropiadas para soportar aplicaciones de negocios

  Para ello se realizara una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema. Los objetivos de control a evaluar serán:

  - o **AI3.2 Protección y Disponibilidad del Recurso de Infraestructura:** Se deberán implementar medidas de control, seguridad y auditabilidad durante cualquier espacio y momento, tanto en el hardware como el software; esto con el fin de proteger los recursos y garantizar su disponibilidad e integridad.

- **DOMINIO - ENTREGAR Y DAR SOPORTE (DS).** En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación. Los procesos que se realizaran y los objetivos de control que se evaluaran son los siguientes.

  - ✓ **Asegurar el Servicio Continuo (DS4).** Objetivo: mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones

    Para ello se tiene un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio. Los objetivos de control a evaluar serán:

    - o **DS4.3 Recursos Críticos de TI:** Las entidades mencionadas deberán poseer un plan de continuidad que identifique que programas, servicios, sistemas operativos, personal, bases de datos, archivos y demás son críticos para el mencionado proceso, así como los tiempos que se necesitarían para recuperar todos estos elementos en caso de una falla amplia.

    - o **DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones:** Las entidades mencionadas deberán proveer un respaldo externo diferente al de las instalaciones donde se realiza el proceso mencionado, todo con el fin de lograr una recuperación rápida en caso de falla mayor. El contenido de dichos respaldos deben determinarse por el grupo de personas involucradas en el proceso mencionado ya que ellos son los responsables de dicho proceso. Las instalaciones deben apegarse a todas las políticas que las entidades mencionadas requieran y tengan dentro de sus estatutos. Además el respaldo debe ser verificado y actualizado periódicamente.

  - ✓ **Garantizar la seguridad de sistemas (DS5).** Objetivo: salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida

    Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados. Los objetivos de control a evaluar serán:

    - o **DS5.1 Administración de la Seguridad de TI:** La administración de seguridad por parte de las entidades mencionadas debe ser llevada a

cabo por la administración que será la encargada de que esta seguridad este en línea con los requerimientos del negocio.

Lo que incluye:

- Identificar los riesgos
- Implementar planes de seguridad
- Actualizar los planes de seguridad
- Monitoreo permanente del plan de seguridad
- Alinear los procedimientos de seguridad (Identificación, Autenticación, Acceso).

o **DS5.2 Plan de Seguridad de TI:** Las entidades mencionadas deberán poseer un plan de seguridad completo, teniendo en cuenta todos los factores que puedan afectar la seguridad, tales factores como infraestructura, cultura de seguridad al interior de las entidades, personal, software y hardware, esto con el fin de que el plan se cumpla a cabalidad junto con sus procedimientos y políticas.

o **DS5.3 Administración de Identidad:** Las entidades mencionadas deben asegurar que todos los usuarios que están involucrados en el proceso de contratación, deberán ser identificables de una única forma. Este usuario deberá ser capaz de identificarse a través de mecanismos de autenticación establecidos por la entidad. Las dependencias mas altas deberán certificar el acceso de los usuarios que lo requieran y estos accesos deberán permanecer en un repositorio para su revisión. Todo este proceso deberá ser reiterado, actualizable y descartable en cualquier momento.

o **DS5.4 Administración de Cuentas del Usuario:** Todas las dependencias que se encuentra involucradas en el proceso mencionado y en si las personas que aquí se ven inmersas, deberán estar supervisadas por su respectivo superior que será capaz de establecer, emitir, suspender, modificar o cerrar las cuentas de los usuarios que así requiera y de los privilegios que este posea, aunque este procedimiento deberá se autorizado y vigilado constantemente. Este tipo de procedimiento se podrá aplicar a cualquier tipo de usuario incluyendo administradores o superadministradores.

o **DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad:** El constante monitoreo de la seguridad tanto física como lógica por parte de los

administradores y en si por parte de quienes están involucrados en el proceso mencionado permitirá a las entidades garantizar la seguridad; por lo tanto el proceso de pruebas, vigilancia y monitoreo deberá ser implementado y mantenido en las entidades en cuestión.

- **DS5.6 Definición de Incidente de Seguridad:** Las entidades mencionadas deberán definir y clasificar los potenciales incidentes de seguridad que se puedan presentar, esto con el fin de que sean tratados de la mejor manera.

- **DS5.7 Protección de la Tecnología de Seguridad:** Las entidades mencionadas deberán establecer un protocolo que garantice que toda la tecnología que se utilice en el proceso mencionado y que tenga fines de seguridad se resistente a ataques y que no revele documentación critica.

- **DS5.9 Prevención, Detección y Corrección de Software Malicioso:** Las entidades deberán garantizar la confiabilidad de la información, y para hacerlo deberán contar con todos los mecanismos pertinentes para la prevención, detección, corrección y eliminación de virus, gusanos, spyware, correo basura y demás conocidos; por lo tanto deberán poseer los antivirus, parches de seguridad y demás que se crean necesarios para llevar a cabo este proceso.

- **DS5.10 Seguridad de la Red:** El cuidado de las redes debe ser prioridad para las entidades mencionadas, ya que hacen parte fundamental de cualquier proceso y mucho más en el de contratación, por lo tanto las entidades mencionadas deberán garantizar el buen uso de estas rede, evitar la intromisión en esta y la caída de las mismas, deberán ayudarse de firewalls, dispositivos de seguridad, segmentación de redes y detección de intrusos lo que hará posible controlar cualquier flujo de información desde y hacia la red.

- **DS5.11 Intercambio de Datos Sensitivos:** Las entidades mencionadas deberán garantizar que el intercambio de información pertinente al proceso se hace por una ruta cien por ciento confiable, con controles que proporcionen autenticidad de contenido, en la que se pruebe el emisor, en la que sea posible probar el receptor y en la que el emisor y el receptor la reciban siempre sin posibilidad de repudio.

- ✓ **Administración de la configuración (DS9).** Objetivo: Dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios

Para ello se realizan controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia. Los objetivos de control a evaluar serán:

- **DS9.1 Repositorio y Línea Base de Configuración:** Deberá existir un repositorio que contenga toda la información relevante del proceso mencionado, así como los cambios tanto de hardware o software que modifiquen cualquier parte de dicho proceso, todo esto con el fin de contar con puntos de restauración validos con los cuales volver atrás en un momento dado.

- **DS9.2 Identificación y Mantenimiento de Elementos de Configuración:** Se deberá establecer protocolos de rastreo de cambios en la información, y se deberán integrar estos procedimientos con la gestión de cambios y de incidentes que hagan mella en la información del proceso en cuestión.

- **DS9.3 Revisión de Integridad de la Configuración:** Las entidades mencionadas deberán garantizar la calidad de software que se utilice en el proceso auditado, se deberá identificar software no licenciado, software mal utilizado o algún otro exceso que pueda perjudicar dicho proceso, todo esto deberá ser reportado para su posterior corrección.

✓ **Administración de Problemas (DS10).** Objetivo: Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder.

Para ello se necesita un sistema de manejo de problemas que registre y dé seguimiento a todos los incidentes, además de un conjunto de procedimientos de escalamiento de problemas para resolver de la manera más eficiente los problemas identificados. Este sistema de administración de problemas deberá también realizar un seguimiento de las causas a partir de un incidente dado. Los objetivos de control a evaluar serán:

- **DS10.2 Rastreo y Resolución de Problemas:** Las entidades deberán prestar todas las capacidades para rastrear de manera efectiva los problemas que se puedan suscitar en el proceso auditado, además deberán presentar un plan de resolución una vez identificado y rastreado dicho inconveniente.

✓ **Administración de Datos (DS11).** Objetivo: Asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento.

Lo cual se logra a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI por lo tanto los objetivos de control a evaluar son:

- **DS11.1 Requerimientos del Negocio para Administración de Datos:** Las entidades deberán garantizar que toda la información que se maneja al interior de sus dependencias se procesa de forma completa, precisa y con los tiempos justos establecidos, además que los resultados que se esperan son de la mayor confiabilidad posible a que esto demuestra transparencia en el proceso.

- **DS11.2 Acuerdos de Almacenamiento y Conservación:** En cualquier proceso que lleven a cabo las entidades mencionadas deberá garantizarse que el archivado, el almacenamiento y la retención de los datos suministrados por exteriores o interiores, se hace con los estándares de seguridad necesarios y exigidos para un desarrollo transparente del proceso.

- **DS11.4 Eliminación:** Toda información sensitiva para los procesos de las entidades mencionadas debe ser tratada con los estándares de seguridad mas altos, sin importar que esta información este en proceso de eliminación ya que hasta que culmine dicho proceso esta información puede causar alteraciones dentro de las entidades mencionadas, por lo tanto dichas entidades deberán garantizar la adecuada eliminación y traspaso de información.

- **DS11.5 Respaldo y Restauración:** Para que el plan de continuidad pueda llevarse a cabo deberá garantizarse por parte de las entidades en mención un procedimiento de respaldo y restauración de cualquier sistema, aplicación o documentación que para este plan de continuidad se requiera.

- **DS11.6 Requerimientos de Seguridad para la Administración de Datos:** Las entidades deberán poner en marcha un protocolo para la administración de datos y para el correcto funcionamiento de la seguridad en esta administración, este protocolo deberá estar presente en el transcurso del recibimiento, procesamiento, almacenamiento y salida de datos.

✓ **Administración de las instalaciones (DS12).** Objetivo: Proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las

instalaciones y contemplen su seguridad física. Los objetivos de control a evaluar son:

- **DS12.2 Medidas de Seguridad Física:** Las entidades deben garantizar la seguridad física de la información, por lo tanto se deberá establecer parámetros de seguridad sin dejar en evidencia la ubicación del equipo crítico para la realización del proceso, así como las áreas importantes para este. Además deberá ser claro el rol de responsabilidades sobre el monitoreo, reporte y resolución de incidentes de seguridad física de las entidades.

- **DS12.3 Acceso Físico:** El acceso a cualquier área o sitio estratégico para la empresa deberá ser controlado por algún procedimiento implementado que permita otorgar, limitar o revocar dicho acceso, no importa el tipo de personal que lo posea. Además cualquier acceso autorizado deberá ser monitoreado permanentemente y además deberá ser documentado.

- **DS12.4 Protección Contra Factores Ambientales:** Las entidades deberán asegurar que se establezcan y sobre todo que se mantengan las adecuadas medidas para la protección contra cualquier factor ambiental excesivo (fuego, polvo, calor, humedad, inundación, electricidad, etc.). Además deberán instalarse los dispositivos necesarios para la detección y posterior control de este tipo de incidentes.

✓ **Administración de la operación (DS13).** Objetivo: Asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada.

Esto se logra a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Para ello, la gerencia deberá establecer y documentar procedimientos para las operaciones de tecnología de información (incluyendo operaciones de red), los cuales deberán ser revisados periódicamente para garantizar su eficiencia y cumplimiento. Los objetivos de control a evaluar son:

- **DS13.4 Documentos Sensitivos y Dispositivos de Salida:** Las entidades deberán establecer adecuados resguardos físicos para la información, estos resguardos deberán poseer un inventario completo con sus respectivos registros, esto se hará para la información más sensitiva y trascendente de las entidades.

- **DS13.5 Mantenimiento Preventivo del Hardware:** Se deberá definir e implementar un procedimiento que garantice el mantenimiento oportuno de la infraestructura de los sistemas esto con el fin de reducir la frecuencia

y el impacto de las fallas, así como la disminución en el desempeño de la entidad.

- **DOMINIO - MONITOREAR Y EVALUAR (ME).** En todas las entidades los procesos necesitan ser evaluados y regulados a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control como integridad y confidencialidad.

  Los objetivos de control que se evaluaran son:

  ✓ **Monitorear y Evaluar el Control Interno (ME2).** Objetivo: Asegurar los logros del control interno de las entidades establecidos para los procesos TI.

  Los objetivos de control que se evaluaran son:

  - **ME2.2 Revisiones de Auditoría:** Se deberán crear mecanismos, procesos y políticas que permitan monitorear y evaluar la eficiencia y efectividad de los controles internos y de revisión hacia el proceso contratación TI.

  - **ME2.4 Auto Evaluación del Control:** Las entidades deberán garantizar la efectividad de los controles sobre los procesos, políticas que regulan el proceso contratación TI, todo esto por medio de autoevaluación constante.

  - **ME2.5 Aseguramiento del Control Interno:** Se deberá garantizar el control interno por medio de revisiones de terceros con parcialidad y objetividad.

  - **ME2.7 Acciones Correctivas:** Las entidades deberán implementar acciones correctivas derivadas de los controles y evaluaciones que se hayan implementado.

3.2.2. Diseño de los elementos de auditoría. Para la realización de la auditoria a las entidades Hospital Universitario Departamental de Nariño E.S.E y al Hospital Civil de Ipiales E.S.E se utilizaron distintos instrumentos de recolección de información los cuales se describen a continuación:

- **Observación Directa.** La Contraloría Departamental de Nariño ha tomado la observación directa como el elemento de auditoría más importante en los procesos que adelanta en todo el Departamento de Nariño.

  Mediante visitas sorpresa se trata de recaudar el mayor volumen de información para su posterior análisis, es así como en las entidades Hospital Universitario

Departamental de Nariño E.S.E y Hospital Civil de Ipiales E.S.E se realizaron dos visitas sorpresa en cada entidad.

- **Entrevistas.** Las entrevistas en las entidades fueron documentadas en video y fueron realizadas por el funcionario de la Contraloría Departamental de Nariño con el apoyo del equipo auditor, cabe aclarar que estas entrevistas se realizaron en el transcurso de la primera inspección, en donde no existía previo aviso de dicha visita, por lo tanto la extracción de información de estas entrevistas se hace con el completo aval de la entidad que ejerce el control sobre las entidades auditadas es decir la Contraloría Departamental de Nariño.

- **Cuadro de definición de fuentes de conocimiento, pruebas de análisis, y pruebas de auditoría**. Con esta herramienta se identifica cual es la información que se necesita para evaluar un determinado proceso dentro de los dominios del COBIT, también se especifica en el cuales son las pruebas de análisis y de ejecución que se deben realizar.

  Los ítems relacionados a continuación son los que describirán el elemento de auditoria.

  REF: Se refiere al ID del elemento.

  ENTIDAD AUDITADA: En este espacio se indicara el nombre de la entidad a la cual se le esta realizando el proceso de auditoria.

  PROCESO AUDITADO: En este espacio se indicara el nombre del proceso objeto de la auditoria, para el caso será Contratación TI.

  RESPONSABLES: En este espacio se indicaran los nombres del equipo auditor que esta llevando a cabo el proceso de auditoria.

  DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: En este espacio se hace una breve referencia al objetivo del proceso seleccionado dentro de los dominios del COBIT que se esta revisando.

  MATERIAL DE SOPORTE: En este espacio se indicara el nombre del material que soporta el proceso, para el caso será COBIT.

  DOMINIO: Espacio reservado para colocar el nombre del dominio de COBIT que se esta evaluando.

  PROCESO: Espacio reservado para el nombre del proceso en especifico que se esta auditando dentro de los dominios del COBIT.

FUENTES DE CONOCIMIENTO: En este espacio se deberá consignar todas las fuentes de donde se extrajo la información para el proceso de auditoria lo que servirá como respaldo del proceso.

REPOSITORIO DE PRUEBAS: Se divide en dos tipos de pruebas:

DE ANÁLISIS: Este espacio esta destinado para describir las pruebas de análisis que se van a realizar para evaluar el proceso especifico que se encuentre en estudio.

DE EJECUCIÓN: Este espacio esta destinado para describir las pruebas de ejecución que se van a realizar para evaluar el proceso especifico que se encuentre en estudio.

Tabla 2: Cuadro de definición de fuentes de conocimiento, pruebas de auditoria, análisis de auditoria

CUADRO DE DEFINICION DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANALISIS DE AUDITORIA	REF	

ENTIDAD AUDITADA	Hospital Universitario Departamental de Nariño.	**PAGINA**		
		1	DE	1
PROCESO AUDITADO	Proceso de Contratación			
RESPONSABLES	Luis Carlos Chaves Yela			
	Ricardo Alexander Cabrera Solarte			
DESCRIPCION DE ACTIVIDAD PRUEBA				
MATERIAL DE SOPORTE	COBIT			
DOMINIO				
PROCESO				

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANALISIS	**DE EJECUCION**

AUDITORES RESPONSABLES:
LUIS CARLOS CHAVES YELA
RICARDO ALEXANDER CABRERA

- **Cuestionario cuantitativo.** El cuestionario cuantitativo mediante una calificación numérica ayuda a identificar la vulnerabilidad de los procesos.

  Los ítems relacionados a continuación son los que describirán el elemento de auditoria.

  REF: Se refiere al ID del elemento.

  ENTIDAD AUDITADA: En este espacio se indicara el nombre de la entidad a la cual se le esta realizando el proceso de auditoria.

  PROCESO AUDITADO: En este espacio se indicara el nombre del proceso objeto de la auditoria, para el caso será Contratación TI.

  RESPONSABLES: En este espacio se indicaran los nombres del equipo auditor que esta llevando a cabo el proceso de auditoria.

  DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: En este espacio se hace una breve referencia al objetivo del proceso seleccionado dentro de los dominios del COBIT que se esta revisando.

  MATERIAL DE SOPORTE: En este espacio se indicara el nombre del material que soporta el proceso, para el caso será COBIT.

  DOMINIO: Espacio reservado para colocar el nombre del dominio de COBIT que se esta evaluando.

  PROCESO: Espacio reservado para el nombre del proceso en especifico que se está auditando dentro de los dominios del COBIT.

  PREGUNTA: Espacio donde se indicara la descripción de la consulta de la cual se indagara.

  SI – NO: Posibilidades de respuesta, cumple, no cumple, o no aplica para la entidad.

  REF: referencia a la evidencia o el hallazgo que se obtuvo después de indagar.

  PORCENTAJE DE RIESGO: Hace referencia a la probabilidad de que el proceso se vea afectado por las acciones de las cuales se está indagando, entre mas alto el porcentaje mayor probabilidad de riesgo tiene el proceso de salir perjudicado.

  El cálculo de este porcentaje se hace de la siguiente forma:

Porcentaje de riesgo parcial = (Total SI * 100) / Total

Porcentaje de riesgo = 100 - Porcentaje de riesgo parcial

Las equivalencias utilizadas para la puntuación serán de uno a cinco, siendo uno el valor mínimo considerado de poca importancia y cinco el máximo considerado de mucha importancia.

Tabla 3: Cuestionario Cuantitativo

CUESTIONARIO CUANTITATIVO	REF	

ENTIDAD AUDITADA	Hospital Universitario Departamental de Nariño		**PAGINA**		
			1	DE	1
PROCESO AUDITADO	Proceso de Contratación				
RESPONSABLES	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO		**PROCESO**			

PREGUNTA	SI	NO	REF
1.			
2.			
3.			
TOTALES			
TOTAL CUESTIONARIO			

PORCENTAJE DE RIESGO:

AUDITORES RESPONSABLES
LUIS CARLOS CHAVES YELA
RICADRO ALEXANDER CABRERA

- **Matriz de Probabilidad de ocurrencia e Impacto según relevancia del proceso.** Esta matriz fue creada para catalogar un riesgo y saber qué clase de daño puede causar un mal procedimiento en el proceso auditado.

  En la matriz existe la columna de probabilidad de ocurrencia donde se pondrá el valor del porcentaje de riesgo según su resultado.

  Luego se deberá clasificar el impacto según la relevancia del proceso, esta clasificación será hecha por el equipo auditor basándose en el conocimiento de la entidad y del proceso auditado.

  Una vez hechos estos procedimientos se podrá clasificar el riesgo para su posterior entendimiento.

MATRIZ DE PROBABILIDAD DE OCURRENCIA E IMPACTO SEGÚN RELEVANCIA DEL PROCESO

Tabla 4: Matriz de probabilidad de ocurrencia e impacto según relevancia del proceso

PROBABILIDAD DE OCURRENCIA				
	60-100%			
	30-60%			
	0-30%			
MATRIZ DE RIESGO		BAJO	MEDIO	ALTO
		IMPACTO SEGÚN RELEVANCIA DEL PROCESO		

- **Manual de navegación de hallazgos.** Los hallazgos que se describen a continuación serán desglosados de la siguiente manera

REF: Se refiere al ID del elemento.

Figura 3: Ref. - Hallazgo

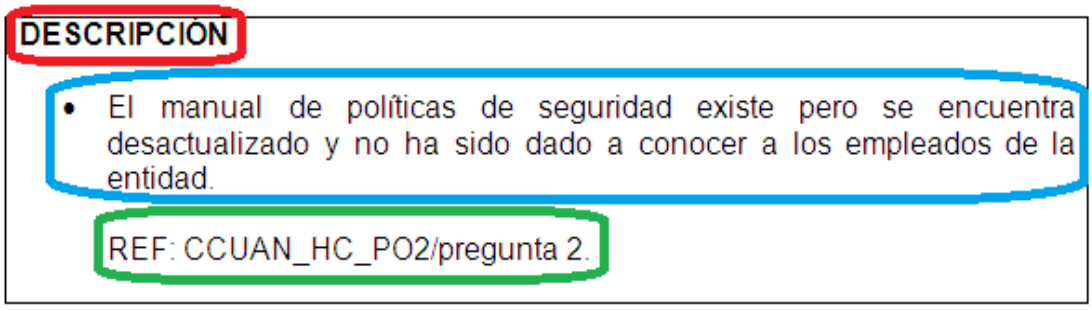
Información General: Hace Referencia a la información relevante de la auditoria tal como el Proceso Auditado (1), los responsables de dicho hallazgo (2), cual es el material que soporta el hallazgo (3), el dominio del material de soporte (4), y el proceso de dicho dominio (5).

Figura 4: Información General Hallazgo

PROCESO AUDITADO	CONTRATACION TI 1	**PÁGINA** 1 DE 2	
RESPONSABLES	LUIS CARLOS CHAVES YELA RICARDO ALEXANDER CABRERA SOLARTE 2		
MATERIAL DE SOPORTE	COBIT 3		
DOMINIO	Planeación y Organización (PO2) 4	**PROCESO**	Definición de la arquitectura de información (PO2) 5

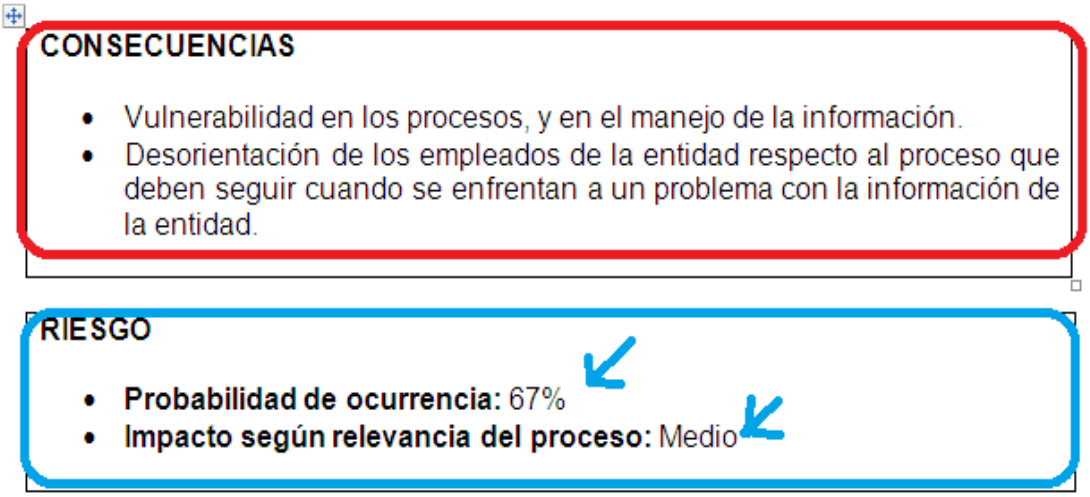
Descripción: Aquí se encontrara la descripción de cada hallazgo, así como la referencia al cuestionario cuantitativo que lo soporta.

Figura 5: Descripción Hallazgo



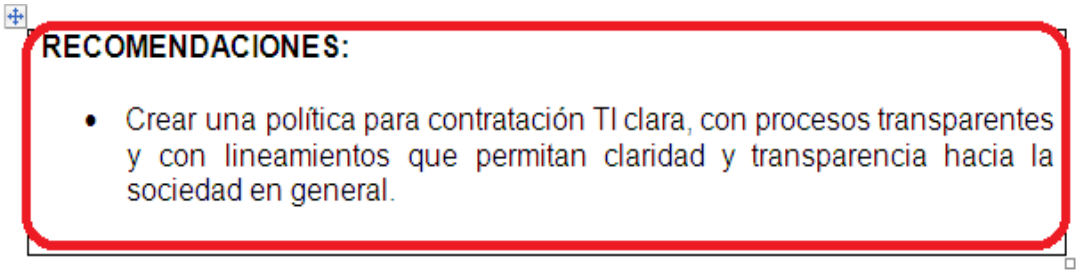
Consecuencias y Riesgos: En este apartado se encuentra la descripción de las consecuencias del hallazgo así como la cuantificación del riesgo encontrado.

Figura 6: Consecuencias y Riesgos



Recomendaciones: En este último apartado se hace una descripción de las recomendaciones que el equipo auditor ha presentado a las entidades auditadas.

Figura 7: Recomendaciones



3.2.3. Hallazgos. A continuación se describirán los hallazgos encontrados en las entidades Hospital Universitario Departamental de Nariño E.S.E y Hospital Civil de Ipiales E.S.E.

- **Dominios y Procesos Auditados.** Los hallazgos encontrados en las entidades se presentaran en el orden de los dominios y procesos auditados los cuales fueron:

1) DOMINIO - PLANIFICACION Y ORGANIZACIÓN (PO)

- Definición de la Arquitectura de Información (PO2).
- Definición de la organización y de las relaciones de TI (PO4)
- Administración de recursos humanos (PO7)
- Evaluación de riesgos (PO9)

2) DOMINIO - ADQUISICION E IMPLEMENTACION (AI)

- Adquisición y mantenimiento del software aplicativo (AI2)
- Adquisición y mantenimiento de la infraestructura tecnológica (AI3)

3) DOMINIO - ENTREGAR Y DAR SOPORTE (DS)

- Asegurar el Servicio Continuo (DS4)
- Garantizar la seguridad de sistemas (DS5)
- Administración de la configuración (DS9)
- Administración de Problemas (DS10)
- Administración de Datos (DS11)
- Administración de las instalaciones (DS12)
- Administración de la operación (DS13)

4) DOMINIO - MONITOREAR Y EVALUAR (ME)

- Monitorear y Evaluar el Control Interno (ME2)

- **Hallazgos Hospital Universitario Departamental de Nariño E.S.E**

Tabla 5: Hallazgo 1 HD

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_01

PROCESO AUDITADO	CONTRATACION TI		**PÁGINA** 1 DE 2		
RESPONSABLES	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO2)	**PROCESO**	Definición de la arquitectura de información (PO2)		

DESCRIPCIÓN

- El manual de políticas de seguridad existe pero se encuentra desactualizado y no ha sido dado a conocer a los empleados de la entidad.

  REF: CCUAN_HC_PO2/pregunta 2.

CONSECUENCIAS

- Vulnerabilidad en los procesos, y en el manejo de la información.
- Desorientación de los empleados de la entidad respecto al proceso que deben seguir cuando se enfrentan a un problema con la información de la entidad.

RIESGO

- **Probabilidad de ocurrencia:** 67%
- **Impacto según relevancia del proceso:** Medio

Tabla 5: Hallazgo 1 HD (Continuación)

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_01

PROCESO AUDITADO	CONTRATACION TI			**PÁGINA** 2 DE 2	
RESPONSABLES	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO2)	**PROCESO**	Definición de la arquitectura de información (PO2)		

RECOMENDACIONES

- Actualizar periódicamente el manual de políticas de seguridad de la información.
- Aplicar los cambios que se crean convenientes al manual de políticas de seguridad de la información.
- Dar a conocer a la planta de personal el manual de políticas de seguridad de la información.
- Realizar seguimiento y reuniones periódicas con el personal para evaluar sus conocimientos respecto al manual de políticas de seguridad de la información

Tabla 6: Hallazgo 2 HD

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E.	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_02

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA** 1 DE 3	
RESPONSABLE	LUIS CARLOS CHAVES YELA RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Organización y de las Relaciones de TI (PO4)		

DESCRIPCIÓN:

- No existe manual de funciones para los trabajadores que interactúan con SICE y SECOP
- No existe planes de reemplazo para funcionarios en caso de ausencia
- No existen políticas adecuadas para la contratación de personal que se involucre con tecnologías de la información
- No se aplican los principios de meritocracia en la entidad
- No todas las personas que cumplan los requisitos pueden ser candidatas al cargo

REF: CCUAN_HD_PO4/pregunta 3, 6, 7, 8

CONSECUENCIAS:

- El mal manejo e ingreso de la información en los sistemas SICE y SECOP por falta de una manual de funciones puede generar retrasos en el ingreso de los datos, lo que podría desencadenar una serie de sanciones por parte de las entidades encargadas de la vigilancia de este sistema.
- Se generarían ingresos de datos anómalos en los sistemas SICE y SECOP
- El servicio de contratación TI se vería abocado a retrasos y fallas generales

Tabla 6: Hallazgo 2 HD (Continuación)

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_02

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA** 2 DE 3	
RESPONSABLE	LUIS CARLOS CHAVES YELA RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Organización y de las Relaciones de TI (PO4)		

CONSECUENCIAS:

- La dependencia hacia funcionarios podría generar paros en el ingreso o manipulación de información
- Se estaría incurriendo en falta de transparencia a la hora de realizar el proceso contratación TI
- Se generaría discriminación ante la sociedad y las personas que a pesar de cumplir con los lineamientos del cargo no tengan la oportunidad de participar de ellos Se generaría discriminación ante la sociedad y las personas que a pesar de cumplir con los lineamientos del cargo no tengan la oportunidad de participar de ellos

RIESGOS:

- **Probabilidad de ocurrencia:** 49%
- **Impacto según relevancia del proceso:** Alto

Tabla 6: Hallazgo 2 HD (Continuación)

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_02

PROCESO AUDITADO	CONTRATACIÓN TI		**PÁGINA** 3 DE 3	
RESPONSABLE	LUIS CARLOS CHAVES YELA RICARDO ALEXANDER CABRERA SOLARTE			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Organización y de las Relaciones de TI (PO4)	

RECOMENDACIONES:

- Se recomienda crear el manual de funciones para los encargados de los sistemas SICE y SECOP
- Se debe eliminar la dependencia hacia los funcionarios por lo tanto cada proceso critico y su información debe ser soportado por al menos dos funcionarios del mismo nivel
- Se debe crear una política completamente clara acerca del proceso contratación TI esto eliminara cualquier manto de duda, esto le dará a la entidad la transparencia que requiere

Tabla 7: Hallazgo 3 HD

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_03

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA** 1 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Administración de recursos humanos (PO7)		

DESCRIPCIÓN:

- No existen políticas ni procedimientos claros para realizar el proceso contratación TI
- No todas las personas que cumplan con los lineamientos del cargo pueden aspirar a el
- No se aplican procesos de selección transparentes ante la sociedad

REF: CCUAN_HD_PO7/pregunta 1,2

CONSECUENCIAS:

- El servicio de contratación TI se vería abocado a retrasos y fallas generales
- Se estaría incurriendo en falta de transparencia a la hora de realizar el proceso contratación TI
- Se generaría discriminación ante la sociedad y las personas que a pesar de cumplir con los lineamientos del cargo no tengan la oportunidad de participar de ellos

Tabla 7: Hallazgo 3 HD (Continuación)

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_03

PROCESO AUDITADO	CONTRATACIÓN TI		**PÁGINA** 2 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA RICARDO ALEXANDER CABRERA SOLARTE			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Administración de recursos humanos (PO7)	

RIESGO:

- **Probabilidad de ocurrencia:** 49%
- **Impacto según relevancia del proceso:** Alto

RECOMENDACIONES:

- Crear una política para contratación TI clara, con procesos transparentes y con lineamientos que permitan claridad y transparencia hacia la sociedad en general.

Tabla 8: Hallazgo 4 HD

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_04

PROCESO AUDITADO	CONTRATACIÓN TI		**PÁGINA** 1 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA RICARDO ALEXANDER CABRERA SOLARTE			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Evaluación de riesgos (PO9)	

DESCRIPCIÓN:

- Los sistemas SICE y SECOP se encuentran totalmente expuestos a fallas por que no existen políticas ni procedimientos para la evaluación de riesgos
- Al momento de realizar cambios en los procedimientos no se tienen en cuenta a los empleados que manejan estos procedimientos
- La entidad no cuenta con un procedimiento claro para el acoplamiento en los cambios externos gubernamentales
- No existe un record de incidentes o inspecciones que den una alternativa para la resolución de conflictos
- No hay un ranking o categorización de riesgos

REF: CCUAN_HD_PO9/pregunta 1,3,7
CCUAN_HD_PO4/pregunta 7

CONSECUENCIAS:

- La exposición a riesgos innecesarios puede desencadenar una falla general en el procedimiento
- Cuando no se tienen en cuenta los requerimientos externos se puede incurrir en una falta de tipo administrativo o penal cuando los requerimientos son gubernamentales

Tabla 8: Hallazgo 4 HD (Continuación)

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_04

PROCESO AUDITADO	CONTRATACIÓN TI		**PÁGINA** 2 DE 2		
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Evaluación de riesgos (PO9)		

CONSECUENCIAS:

- Cuando no se posee una categorización clara de los riesgos no se puede saber con claridad cual de ellos tendrá mas impacto en los procesos o cual podría dejar totalmente inutilizado dicho proceso

RIESGOS:

- **Probabilidad de ocurrencia:** 42%
- **Impacto según relevancia del proceso:** Medio

RECOMENDACIONES:

- Se recomienda tener en cuenta los requerimientos externos de cambio sin importar de que tipo sean
- Se debe crear una categorización clara de riesgos para su control y evaluación y posteriormente hacer un archivo de los mismos para su consulta que permita la oportuna resolución de riesgos

Tabla 9: Hallazgo 5 HD

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_05

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA** 1 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e implementación	**PROCESO**	Adquisición y mantenimiento del software aplicativo (AI2)		

DESCRIPCIÓN:

- En la entidad no existe un plan de depuración de datos
- En la entidad no existe un manual para el manejo de los sistemas SICE y SECOP

REF: CCUAN_HD_AI2/pregunta 2, 3

CONSECUENCIAS:

- La no depuración de datos generan corrupción en la información, corrupción en el proceso y por ende degeneraran en fallas graves y en algunos casos generales
- El mal manejo e ingreso de la información en los sistemas SICE y SECOP por falta de una manual de manejo puede generar retrasos en el ingreso de los datos, lo que podría desencadenar una serie de sanciones por parte de las entidades encargadas de la vigilancia de este sistema.
- Se podrían generar ingresos de datos anómalos en los sistemas SICE y SECOP

Tabla 9: Hallazgo 5 HD (Continuación)

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E.	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_05

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA** 2 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e implementación	**PROCESO**	Adquisición y mantenimiento del software aplicativo (AI2)		

RIESGOS:

- **Probabilidad de ocurrencia:** 67%
- **Impacto según relevancia del proceso:** Medio

RECOMENDACIONES:

- Se debe crear y poner en marcha un plan de depuración de datos
- Se debe crear y poner en marcha un manual adecuado para el manejo de los sistemas SICE y SECOP

Tabla 10: Hallazgo 6 HD

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_06

PROCESO AUDITADO	CONTRATACIÓN TI		**PÁGINA** 1 DE 3		
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e implementación	**PROCESO**	Adquisición y mantenimiento de la infraestructura tecnológica (AI3)		

DESCRIPCIÓN:

- Las políticas y procedimientos para la adquisición de hardware no se encuentran bien fundamentadas.
- Las políticas y procedimientos para la adquisición de hardware no se encuentran documentadas
- Las políticas y procedimientos para la adquisición de hardware no son conocidas por los funcionarios
- Los procedimientos para el mantenimiento preventivo de los equipos de la entidad no son los mejores ni los mas óptimos
- Las políticas y procedimientos de mantenimiento preventivo de los equipos de la entidad no se encuentra documentada por completo
- Las políticas y procedimientos de mantenimiento preventivo de los equipos de la entidad no son de conocimiento de toda la planta de funcionarios
- Las reparaciones son llevadas a cabo por los mismos funcionarios sin importar de que tipo sean
- Las políticas y procedimientos para la adquisición de software no se encuentran bien fundamentadas.
- Las políticas y procedimientos para la adquisición de software no se encuentran documentadas
- Las políticas y procedimientos para la adquisición de software no son conocidas por los funcionarios

REF: CCUAN_HD_AI3/pregunta 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27

Tabla 10: Hallazgo 6 HD (Continuación)

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_06

PROCESO AUDITADO	CONTRATACIÓN TI		**PÁGINA**		
			2	DE	3
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e implementación	**PROCESO**	Adquisición y mantenimiento de la infraestructura tecnológica (AI3)		

CONSECUENCIAS:

- Al no existir políticas de adquisición de hardware se puede incurrir en gastos redundantes, que derivan en el detrimento del patrimonio publico al ser una entidad regulada por el estado
- Al no existir políticas de adquisición de software se puede incurrir en gastos redundantes, que derivan en el detrimento del patrimonio publico al ser una entidad regulada por el estado
- Al no existir buenas políticas para el mantenimiento preventivo de los equipos, este podría quedar mal hecho lo que generaría gastos posteriores
- Ya que los encargados de los arreglos a los equipos no son las personas mas idóneas, estos arreglos pueden causar un daño mucho mas grave en estos equipos lo que generaría gastos mayores

RIESGOS:

- **Probabilidad de ocurrencia:** 31%
- **Impacto según relevancia del proceso:** Alto

Tabla 10: Hallazgo 6 HD (Continuación)

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_06

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA** 3 DE 3	
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e implementación	**PROCESO**	Adquisición y mantenimiento de la infraestructura tecnológica (AI3)		

RECOMENDACIONES:

- Se debe crear y poner en marcha políticas y procedimientos para la adquisición de hardware
- Se debe crear y poner en marcha políticas y procedimientos para la adquisición de software
- Se debe modificar y poner en marcha la política y el procedimiento para el mantenimiento preventivo y correctivo de los equipos

Tabla 11: Hallazgo 7 HD

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_07

PROCESO AUDITADO	CONTRATACIÓN TI		**PÁGINA** 1 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA			
	RICARDO ALEXANDER CABRERA SOLARTE			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Asegurar el Servicio Continuo (DS4)	

DESCRIPCIÓN:

- Existen estrategias para garantizar el proceso contratación TI pero estas no son las mas optimas ni se encuentran actualizadas
- No existe un plan adecuado para la recuperación ante desastres
- No se ha programado un plan para la distribución de la documentación de los planes de riesgo
- En el plan de continuidad no se contempla el impacto al proceso contratación TI
- Los funcionarios no conocen las estrategias de actuación frente a un desastre
- La información se encuentra centralizada lo que genera un caos de datos si se presentara una pérdida

REF: CCUAN_HD_DS4/pregunta 2, 3, 4, 5, 6, 7

CONSECUENCIAS:

- La entidad seria incapaz de realizar la recuperación de información si se presentara una eventualidad en su contra
- No se podría garantizar la continuidad de los procesos
- Perdida total de la información clave para el proceso en caso de eventualidad en la entidad

Tabla 11: Hallazgo 7 HD (Continuación)

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_07

PROCESO AUDITADO	CONTRATACIÓN TI		**PÁGINA** 2 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA			
	RICARDO ALEXANDER CABRERA SOLARTE			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Asegurar el Servicio Continuo (DS4)	

RIESGOS:

- **Probabilidad de ocurrencia:** 86%
- **Impacto según relevancia del proceso:** Medio

RECOMENDACIONES:

- Crear un plan de recuperación de datos en caso de desastres
- Dar a conocer el plan de recuperación de datos en caso de desastres a todo el personal de la entidad
- Descentralizar la información

Tabla 12: Hallazgo 8 HD

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_08

PROCESO AUDITADO	CONTRATACIÓN TI	**PÁGINA** 1 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA		
	RICARDO ALEXANDER CABRERA SOLARTE		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Garantizar la seguridad de sistemas (DS5)

DESCRIPCIÓN:

- Existe una política de seguridad lógica en la entidad pero esta no esta bien fundamentada ni actualizada
- Existen políticas control de acceso pero no se encuentran actualizadas ni están correctamente diseñadas
- Las políticas de control de acceso no son del todo conocidas, ni puestas en practica por los funcionarios de la entidad
- El software que defiende las terminales de ataques de virus, troyanos, gusanos y demás no se encuentra actualizado correctamente y en algunos casos carece de licencia

REF: CCUAN_HD_DS5/pregunta 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 12, 13, 14

CONSECUENCIAS:

- La falta de políticas de seguridad puede generar cese de actividades en el proceso contratación TI, ya que se puede presentar malversación de la información o perdida de esta
- Al no conocer las políticas de control de acceso y al no ponerlas en funcionamiento se puede generar un saqueo de información o manipulación de la misma

Tabla 12: Hallazgo 8 HD (Continuación)

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_08

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA** 2 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Garantizar la seguridad de sistemas (DS5)		

CONSECUENCIAS:

- Si el software que defiende las terminales de trabajo no se encuentra trabajando al cien por ciento es posible que se pierda información sumamente valiosa lo que puede generar un cese de actividades en el proceso contratación TI

RIESGOS:

- **Probabilidad de ocurrencia:** 20%
- **Impacto según relevancia del proceso:** Alto

RECOMENDACIONES:

- Crear y poner en marcha una política clara y contundente de seguridad lógica
- Actualizar y licenciar según sea el caso el software que defiende las terminales de trabajo de la entidad

Tabla 13: Hallazgo 9 HD

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E.	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_09

PROCESO AUDITADO	CONTRATACIÓN TI		**PÁGINA** 1 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA			
	RICARDO ALEXANDER CABRERA SOLARTE			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de la configuración (DS9)	

DESCRIPCIÓN:

- No hay claridad en las políticas respecto al software que la entidad permite instalar en sus terminales
- No hay políticas procedimientos claros respecto a hardware permitido por la entidad
- No hay documentación de las políticas que regulan la instalación o utilización de hardware y software
- No hay controles hacia los funcionarios que podrían utilizar software y hardware desconocido

REF: CCUAN_HD_DS9/pregunta 3, 4, 5, 6, 7, 8

CONSECUENCIAS:

- Podría existir la manipulación, extracción, o eliminación de información por parte de personas malintencionadas externas o internas a la entidad
- Puede existir un daño en los equipos que controlan la información critica en la entidad

Tabla 13: Hallazgo 9 HD (Continuación)

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_09

PROCESO AUDITADO	CONTRATACIÓN TI		**PÁGINA** 2 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA			
	RICARDO ALEXANDER CABRERA SOLARTE			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de la configuración (DS9)	

RIESGOS:

- **Probabilidad de ocurrencia:** 61%
- **Impacto según relevancia del proceso:** Alto

RECOMENDACIONES:

- Crear y poner en marcha una política clara con respecto al software y hardware que los funcionarios pueden instalar y manipular en los equipos de la entidad
- Realizar los controles necesarios y regulares hacia los funcionarios y equipos con respecto a hardware y software que puede o no ser utilizado e instalado en la entidad

Tabla 14: Hallazgo 10 HD

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_10

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA** 1 DE 1	
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de Problemas (DS10)		

DESCRIPCIÓN:

- No hay estrategias que permitan identificar y rastrear posibles riesgos en el proceso contratación TI

  REF: CCUAN_HD_DS10/pregunta 1, 2, 3, 4

CONSECUENCIAS:

- Al no existir estrategias de rastreo de riesgos es imposible saber a que se enfrenta la entidad realmente en cuestión de manejo seguro de la información

RIESGOS:

- **Probabilidad de ocurrencia:** 100%
- **Impacto según relevancia del proceso:** Medio

RECOMENDACIONES:

- Crear estrategias que permitan identificar y rastrear posibles riesgos en el proceso contratación TI

Tabla 15: Hallazgo 11 HD

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E.	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_11

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA** 1 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de Datos (DS11)		

DESCRIPCIÓN:

- No existe la documentación de las políticas de copias de seguridad de la información
- No se encuentran definidos los procedimientos para los periodos de retención y los términos de almacenamiento de la información
- La información es almacenada en el archivo central de la entidad, y descansa solo en ese lugar lo que acarrea problemas ante posibles desastres o filtraciones de información

REF: CCUAN_HD_DS11/pregunta 4, 6, 7, 8, 9, 11, 12

CONSECUENCIAS:

- Al no existir documentación de las políticas de copias de seguridad, estas copias se realizan empíricamente y no son de la mejor calidad y podrían causar daños en el proceso contratación TI
- Al descansar las copias en la misma entidad se puede presentar la perdida total o parcial de esta lo que causaría el cese del proceso contratación TI

Tabla 15: Hallazgo 11 HD (Continuación)

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_11

PROCESO AUDITADO	CONTRATACIÓN TI		**PÁGINA** 2 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA			
	RICARDO ALEXANDER CABRERA SOLARTE			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de Datos (DS11)	

RIESGOS:

- **Probabilidad de ocurrencia:** 41%
- **Impacto según relevancia del proceso:** Alto

RECOMENDACIONES:

- Crear la documentación de las políticas de copias de seguridad
- Crear un plan de archivo exterior con todas las políticas y procedimientos que esto implica

Tabla 16: Hallazgo 12 HD

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_12

PROCESO AUDITADO	CONTRATACIÓN TI		**PÁGINA** 1 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA RICARDO ALEXANDER CABRERA SOLARTE			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de las instalaciones (DS12)	

DESCRIPCIÓN:

- Las políticas de seguridad para el ingreso a la entidad se encuentran bien fundamentadas pero existen algunas fallas cuando el ingreso se hace por medio de algún vehículo
- La entidad no cuenta con un centro de cómputo adecuado, y no posee la seguridad necesaria.
- En el lugar donde se están llevando a cabo las tareas de centro de cómputo no se cuentan con las condiciones adecuadas de espacio, iluminación, ventilación, seguridad física y demás necesarias para un buen funcionamiento.

REF: CCUAN_HD_DS12/pregunta 2, 4, 5

CONSECUENCIAS:

- La falta de políticas bien fundamentadas puede generar robos de información o equipo de hardware necesario para solventar el proceso contratación TI
- La falta de un centro de cómputo adecuado puede generar la mala manipulación de la información, la fuga de esta y puede provocar un cese de actividades en el proceso.

Tabla 16: Hallazgo 12 HD (Continuación)

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_12

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA** 2 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de las instalaciones (DS12)		

RIESGOS:

- **Probabilidad de ocurrencia:** 24%
- **Impacto según relevancia del proceso:** Alto

RECOMENDACIONES:

- Se recomienda extender las políticas de seguridad para el ingreso a la entidad, y acrecentarlas cuando se trata de vehículos automotores
- Se recomienda crear un centro de cómputo con las condiciones necesarias para asegurar las condiciones de trabajo y de los procesos.

Tabla 17: Hallazgo 13 HD

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_13

PROCESO AUDITADO	CONTRATACIÓN TI		**PÁGINA** 1 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA			
	RICARDO ALEXANDER CABRERA SOLARTE			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de la operación (DS13)	

DESCRIPCIÓN:

- No existen estrategias que garanticen el adecuado resguardo de la información
- No existe un adecuado inventario de estos resguardos de información

REF: CCUAN_HD_DS13/pregunta 1, 2, 3, 4, 5

CONSECUENCIAS:

- Al no existir estrategias que garanticen el adecuado resguardo de la información se puede correr el riesgo de perdida total o parcial de la información que soporta el proceso contratación TI
- Al no existir resguardo de la información cualquier perdida puede causar el cese de las actividades parcial o total del proceso contratación TI

Tabla 17: Hallazgo 13 HD (Continuación)

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_13

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA** 2 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de la operación (DS13)		

RIESGOS:

- **Probabilidad de ocurrencia:** 100%
- **Impacto según relevancia del proceso:** Alto

RECOMENDACIONES:

- Se debe crear y poner en marcha las estrategias que garanticen el resguardo de la información sensible para el proceso
- Se debe crear un adecuado resguardo para la información sensible del proceso
- Se debe crear una estrategia que garantice el adecuado mantenimiento de la infraestructura que maneja el proceso contratación TI

Tabla 18: Hallazgo 14 HD

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_14

PROCESO AUDITADO	CONTRATACION TI			**PÁGINA** 1 DE 2	
RESPONSABLES	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
FECHA					
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Monitorear y evaluar	**PROCESO**	Monitorear y Evaluar el Control Interno (ME2)		

DESCRIPCIÓN:

- No existe un monitoreo constante de actividades dentro del proceso contratación TI, que pretendan brindar mayor seguridad física y lógica a los activos físicos o de información que soportan el mencionado proceso.

CONSECUENCIAS:

- Se puede generar perdida total o parcial de información relevante para el soporte del proceso contratación TI
- La falta de monitoreo puede generar fuga de información
- La falta de políticas y de conocimiento de las mismas produciría caos en el manejo de la información si esta se encontrara expuesta a algún riesgo

REF: CCUAN_HD_ME2/pregunta 1, 2, 3, 4

RIESGO:

- **Probabilidad de ocurrencia:** 100%
- **Impacto según relevancia del proceso:** Bajo

Tabla 18: Hallazgo 14 HD (Continuación)

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	**HALLAZGO HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO**	**REF** HHD_14

PROCESO AUDITADO	CONTRATACION TI			**PÁGINA** 2 DE 2	
RESPONSABLES	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
FECHA					
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Monitorear y evaluar	**PROCESO**	Monitorear y Evaluar el Control Interno (ME2)		

RECOMENDACIONES:

- Crear las políticas de monitoreo que permitan brindar mayor seguridad física y lógica a los activos de tecnología de la información de los sistemas SICE y SECOP

- **Hallazgos Hospital Civil de Ipiales E.S.E**

Tabla 19: Hallazgo 1 HC

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_O1

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA**	
				1	DE 1
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización	**PROCESO**	Definición de la arquitectura de información (PO2)		

DESCRIPCIÓN:

- No existe un procedimiento establecido para mantener actualizado el Manual de Políticas de seguridad de la información.

  REF: CCUAN_HC_PO2/pregunta 2.

CONSECUENCIAS:

- Cuando se realice algún cambio en el sistema o en la red los usuarios conocerán el funcionamiento actual del proceso de la información.

RIESGO:

- **Probabilidad de ocurrencia:** 33.33%
- **Impacto según relevancia del proceso:** Alto

RECOMENDACIONES:

- Establecer un proceso para mantenerlo actualizado el Manual de Políticas de seguridad de la información.

Tabla 20: Hallazgo 2 HC

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_O2

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA**	
				1 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización	**PROCESO**	Definición de la Organización y de las Relaciones de TI (PO4)		

DESCRIPCIÓN:

- No existe un manual de funciones para los empleados que interactúan con el SICE y SECOP, además de un procedimiento para realizar la contratación del personal que se involucre con tecnologías de información. No existe un plan de contingencia para reemplazar funcionarios en caso de ausencia.

  REF: CCUAN_HC_PO4/preguntas 2, 3, 6, 7 ,8.

CONSECUENCIAS:

- La no existencia de un manual de funciones para los empleados que interactúan con el SICE y SECOP puede generar que se presenten inconsistencias en la información que se registre en estos sistemas, mal manejo de los mismos.
- El no estar definido un procedimiento para realizar la contratación del personal que se involucre con tecnologías de información puede generar que no se contrate a personal idóneo para realizar las actividades que el sistema requiera y que no se tengan en cuenta los requisitos que estas personas deban cumplir para poder asumir estos cargos, afectando esto la Definición de la Organización y de las Relaciones de TI.

RIESGO:

- **Probabilidad de ocurrencia:** 49%
- **Impacto según relevancia del proceso:** Medio.

Tabla 20: Hallazgo 2 HC (Continuación)

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_O2

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA**	
				2	DE 2
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización	**PROCESO**	Definición de la Organización y de las Relaciones de TI (PO4)		

RECOMENDACIONES:

- Realizar un manual de funciones para los empleados que interactúan con el SICE y SECOP donde se especifique:

    - Una identificación clara de los roles o cargos que los funcionarios deberán desempeñar.
    - Las responsabilidades y roles para los funcionarios que interactúan con estos sistemas.
    - Las funciones que los funcionarios deben desempeñar de acuerdo con los roles y responsabilidades que se les fue asignado.
    - La descripción de los perfiles que deben poseer los funcionarios que interactúan con los estos sistemas.
    - La descripción de los procesos que los usuarios de los sistemas SICE y SECOP deben seguir para garantizar la seguridad de la información.

Tabla 21: Hallazgo 3 HC

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_O3

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA**	
				1	DE 1
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización	**PROCESO**	Administración de recursos humanos (PO7)		

DESCRIPCIÓN:

- No existen políticas y procedimientos para realizar la contratación del personal que se involucre con tecnologías de información.

  REF: CCUAN_HC_PO2/preguntas 1, 2.

CONSECUENCIAS:

- El no existir políticas y procedimientos para realizar la contratación del personal que se involucre con tecnologías de información puede generar que no se cuente con un equipo de personas adecuado afectando el proceso de contratación TI

RIESGO:

- **Probabilidad de ocurrencia:** 80%
- **Impacto según relevancia del proceso:** medio

RECOMENDACIONES:

- Elaborar un documento donde se describan las políticas y procedimientos para realizar la contratación del personal que se involucre con tecnologías de información.

Tabla 22: Hallazgo 4 HC

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_O4

PROCESO AUDITADO	CONTRATACIÓN TI		**PÁGINA**	
			1 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA			
	RICARDO ALEXANDER CABRERA SOLARTE			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización	**PROCESO**	Evaluación de riesgos (PO9)	

DESCRIPCIÓN:

- No existen políticas y procedimientos en relación a la evaluación de riesgos en los sistemas SICE y SECOP. No existe un marco referencial y procedimientos para la evaluación de riesgos, además de un plan de acción contra riesgos. No se realiza periódicamente una evaluación de riesgos en la contratación TI de las entidades mencionadas. No existe un plan de acción contra riesgos. No existen políticas o procedimientos para la adquisición de pólizas de seguros para el manejo de los riesgos.

  REF: CCUAN_HC_PO9/preguntas: 1, 2, 3, 4, 5, 6, 7, 8, 9.

CONSECUENCIAS:

- Al no existir un marco referencial y procedimientos para la evaluación de riesgos los activos que están involucrados en el proceso de contratación TI, están expuestos a sufrir daños físicos y lógicos, ocasionados por la ocurrencia de un evento potencialmente catastrófico sobre el cual no se ejerce ningún tipo de control.

RIESGO:

- **Probabilidad de ocurrencia:** 100%
- **Impacto según relevancia del proceso:** medio

Tabla 22: Hallazgo 4 HC (Continuación)

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_O4

PROCESO AUDITADO	CONTRATACIÓN TI		**PÁGINA**	
			2 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA			
	RICARDO ALEXANDER CABRERA SOLARTE			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización	**PROCESO**	Evaluación de riesgos (PO9)	

RECOMENDACIONES:

- Desarrollar un marco referencial y procedimientos para la evaluación de riesgos, donde se especifique:

  - Aspectos relacionados con la actualización o mantenimiento del hardware e infraestructura de red.
  - Cambios en los requerimientos de los usuarios.
  - Cambios en los requerimientos externos gubernamentales.
  - Auditorias, inspecciones, o incidentes anteriores ocurridos en relación a las tecnologías de información del Hospital.

- Elaborar un plan de acción contra riesgos y establecer políticas o procedimientos para la adquisición de pólizas de seguros para el manejo de los riesgos.

Tabla 23: Hallazgo 5 HC

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_05

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA**	
				1 DE 1	
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e implementación	**PROCESO**	Adquisición y mantenimiento del software aplicativo (AI2)		

DESCRIPCIÓN:

- No existe un manual para el manejo de SECOP y SICE y no existe algún plan de depuración de datos.

  REF: CCUAN_HC_AI2/preguntas: 2, 3.

CONSECUENCIAS:

- Al no existir un manual para el manejo de SECOP y SICE se presenta una mala utilización de estos sistemas generando alarmas y fallos que entorpecen el proceso de contratación TI.

RIESGO:

- **Probabilidad de ocurrencia:** 66.67%
- **Impacto según relevancia del proceso:** Alto

RECOMENDACIONES:

- Elaborar un manual para el manejo de SECOP y SICE y un plan de depuración de datos.

Tabla 24: Hallazgo 6 HC

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_06

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA**	
				1 DE 3	
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e implementación	**PROCESO**	Adquisición y mantenimiento de la infraestructura tecnológica (AI3)		

DESCRIPCIÓN:

- No existen políticas y procedimientos para la adquisición de hardware aunque se tiene en cuenta la opinión de un experto en el equipo que se va a adquirir.
- No existen políticas y procedimientos para la adquisición de software aunque se realiza un proceso adecuado a la hora de adquirirlo.
- No existen políticas para llevar a cabo el mantenimiento preventivo o correctivo de los equipos de cómputo.
- Dentro del equipo de mantenimiento no existen especialistas en reparaciones eléctricas

REF: CCUAN_HC_AI3/preguntas: 1, 3, 4, 5, 7, 8, 11, 13, 14, 15, 17, 18, 19. 21, 22, 24, 26, 27.

CONSECUENCIAS:

- Aunque se tiene en cuenta la opinión de un experto a la hora de adquirir hardware o software, en la entidad no existen políticas que describan el proceso que se debe llevar a cabo cuando se necesite adquirir alguno de estos elementos, por lo tanto los empleados no tienen claro el proceso a seguir para solicitar un artículo o programa, esto genera que este proceso se pueda llevar a cabo irregularmente.
- Al no encontrarse en la entidad políticas para llevar a cabo el mantenimiento preventivo o correctivo de los equipos de cómputo se puede generar el deterioro y daño de las terminales de trabajo de los usuarios que interactúan con el proceso de contratación TI.

Tabla 24: Hallazgo 6 HC (Continuación)

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF** **HHC_06**

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA** 2 DE 3	
RESPONSABLE	LUIS CARLOS CHAVES YELA RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e implementación	**PROCESO**	Adquisición y mantenimiento de la infraestructura tecnológica (AI3)		

RIESGO:

- **Probabilidad de ocurrencia:** 33%
- **Impacto según relevancia del proceso:** medio

RECOMENDACIONES:

- Desarrollar políticas y procedimientos para la adquisición de hardware donde se especifiquen:
  - La realización de una solicitud de compra formal y por escrito del hardware
  - La solicitud describe las características que debe poseer el hardware
  - La solicitud describe la necesidad de adquisición del hardware
  - La cotización de diferentes proveedores del hardware a comprar
  - Análisis de las propuestas de los proveedores
  - Se elige la propuesta de adquisición de hardware más favorable para la entidad

Tabla 24: Hallazgo 6 HC (Continuación)

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_06

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA**	
				3	DE 3
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e implementación	**PROCESO**	Adquisición y mantenimiento de la infraestructura tecnológica (AI3)		

RECOMENDACIONES:

- Desarrollar políticas y procedimientos para la adquisición de software donde se especifiquen:

  - La realización de una solicitud de compra formal y por escrito del software
  - La solicitud describe las características que debe poseer el software
  - La solicitud describe la necesidad de adquisición del software
  - La realización del proceso de análisis para determinar si se compra software comercial o se contrata la realización de software a la medida
  - El software comercial que se adquiera deberá ser legal y contar con su respectiva licencia
  - Si se contrata el desarrollo se contempla información sobre la plataforma en la que sea desarrollado el software.

- Elaborar políticas para llevar a cabo el mantenimiento preventivo o correctivo de los equipos de cómputo.

Tabla 25: Hallazgo 7 HC

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF** **HHC_07**

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA** 1 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Asegurar el Servicio Continuo (DS4)		

DESCRIPCIÓN:

- En el manual de contratación no se tiene en cuenta planes de recuperación ante desastres, definición del esquema de análisis de riesgo, documentación y distribución de los planes de riesgo.
- No existe un plan de continuidad que contemple la identificación de los procesos críticos y el análisis de impacto

REF: CCUAN_HC_DS4/preguntas: 2, 3, 4, 5, 6, 7.

CONSECUENCIAS:

- Al no tener en cuenta planes de recuperación ante desastres, definición del esquema de análisis de riesgo, documentación y distribución de los planes de riesgo, puede generar el cese total de actividades, en caso de presentarse un evento potencialmente catastrófico. Lo mismo sucede por no tener un plan de continuidad que contemple la identificación de los procesos críticos y el análisis de impacto, debido a que no se le puede dar prioridad a este tipo de procesos porque son totalmente desconocidos por el personal que labora en la entidad.

RIESGO:

- **Probabilidad de ocurrencia:** 86%
- **Impacto según relevancia del proceso:** Bajo

Tabla 25: Hallazgo 7 HC (Continuación)

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_07

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA**	
				2	DE 2
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Asegurar el Servicio Continuo (DS4)		

RECOMENDACIONES:

- Incluir dentro del manual de contratación:

  - Planes de recuperación ante desastres
  - Definición del esquema de análisis de riesgo.
  - Documentación y distribución de los planes de riesgo

- Elaborar un plan de continuidad que contemple la identificación de los procesos críticos y el análisis de impacto donde se especifique:

  - Guía de cómo utilizar el plan
  - Procedimientos de evacuación del personal
  - Tipos de condiciones para ser declarado un desastre
  - Identificación de los elementos críticos que deben ser recuperados tras un desastre
  - Explicación de los procedimientos de emergencia que se deben realizar en caso de desastre

Tabla 26: Hallazgo 8 HC

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_08

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA**	
				1	DE 2
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Garantizar la seguridad de sistemas (DS5)		

DESCRIPCIÓN:

- Dentro de las políticas de seguridad lógica en la entidad no se tiene en cuenta:

  - Reportes y revisión de las violaciones e incidentes de seguridad
  - Administración de llaves criptográficas
  - Detección, resolución y comunicación sobre los virus
  - Clasificación y propiedad de los datos
  - No existen políticas de control de contraseñas.

  REF: CCUAN_HC_DS5/preguntas: 2, 3, 4, 5, 6, 7, 8, 9.

CONSECUENCIAS:

- La información critica de la empresa se ve insegura al no tener políticas de control de contraseñas y no tener en cuenta dentro de las políticas de seguridad lógica:

  - Reportes y revisión de las violaciones e incidentes de seguridad
  - Administración de llaves criptográficas
  - Detección, resolución y comunicación sobre los virus
  - Clasificación y propiedad de los datos.

Tabla 26: Hallazgo 8 HC (Continuación)

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_08

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA**	
				2	DE 2
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Garantizar la seguridad de sistemas (DS5)		

RIESGO:

- Probabilidad de ocurrencia: 62%
- Impacto según relevancia del proceso: Alto

RECOMENDACIONES:

- Incluir dentro de las políticas de seguridad lógica en la entidad:
  - Reportes y revisión de las violaciones e incidentes de seguridad
  - Administración de llaves criptográficas
  - Detección, resolución y comunicación sobre los virus
  - Clasificación y propiedad de los datos
- Elaborar políticas de control de contraseñas donde se especifique:
  - Cambio periódico de contraseña
  - Longitud adecuada de contraseña
  - Combinaciones alfanuméricas obligatorias
  - Protección de las contraseñas

Tabla 27: Hallazgo 9 HC

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_09

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA**	
				1 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de la configuración (DS9)		

DESCRIPCIÓN:

- No existe un inventario de la configuración de las terminales de trabajo de los usuarios que interactúan con el SICE y SECOP.

  REF: CCUAN_HC_DS9/preguntas: 1, 2, 8.

CONSECUENCIAS:

- Si no existe un inventario de la configuración de las terminales de trabajo se pueden generar demoras en el restablecimiento de los servicios que se presta en caso de tener que realizar actividades críticas de mantenimiento (formatear, reinstalar sistema operativo, etc.)

RIESGO:

- **Probabilidad de ocurrencia:** 58%
- **Impacto según relevancia del proceso:** Medio

Tabla 27: Hallazgo 9 HC (Continuación)

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_09

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA**	
				2	DE 2
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de la configuración (DS9)		

RECOMENDACIONES:

- Desarrollar un inventario de la configuración de las terminales de trabajo de los usuarios que interactúan con el SICE y SECOP donde se observe claramente:

  - La configuración referente al Sistema Operativo de las terminales.
  - La configuración del software instalado en las diferentes terminales.
  - Información referente a las licencias de los diferentes programas instalados en las terminales de trabajo.
  - La configuración del hardware instalado.

Tabla 28: Hallazgo 10 HC

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF** **HHC_10**

PROCESO AUDITADO	CONTRATACIÓN TI		**PÁGINA** 1 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA RICARDO ALEXANDER CABRERA SOLARTE			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de Problemas (DS10)	

DESCRIPCIÓN:

- No existen estrategias que garanticen el rastreo de problemas en el proceso contratación TI.

  REF: CCUAN_HC_DS10/preguntas: 1, 2, 3, 4.

CONSECUENCIAS:

- Cuando no se cuenta con estrategias que garanticen el rastreo de problemas en el proceso contratación TI, no se podría corregir o solucionar estos problemas y se podría reincidir a la hora de repetir este proceso.

RIESGO:

- Probabilidad de ocurrencia: 100%
- Impacto según relevancia del proceso: medio

Tabla 28: Hallazgo 10 HC (Continuación)

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_10

PROCESO AUDITADO	CONTRATACIÓN TI		**PÁGINA**	
			2 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA			
	RICARDO ALEXANDER CABRERA SOLARTE			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de Problemas (DS10)	

RECOMENDACIONES:

- Establecer estrategias que garanticen el rastreo de problemas en el proceso contratación TI donde se describa:

    - Planes de recuperación.
    - Definición del esquema de análisis de riesgo.
    - Documentación y distribución de los planes de riesgo.
    - Resolución de problemas rastreados.

Tabla 29: Hallazgo 11 HC

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_11

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA**	
				1 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de Datos (DS11)		

DESCRIPCIÓN:

- No se realizan copias de seguridad de los datos que manejan SICE Y SECOP.
- En las políticas para la realización de las copias de seguridad no se tiene en cuenta:

  - Realización diaria de copias de seguridad de la información que se actualiza frecuentemente.
  - Realización semanal de copias de seguridad de la información menos sensible
  - Conservar al menos una semana la copia de seguridad diaria
  - Conservar al menos un mes la copia de seguridad semanal
  - Conservar una copia de cada mes al menos durante un año
  - Conservar una copia anual de toda la información.

  REF: CCUAN_HC_DS11/preguntas: 1, 3, 4, 7, 9.

CONSECUENCIAS:

- Si no existen políticas para realizar copias de seguridad, los empleados o encargados de realizarlas lo hagan de forma empírica y sin seguir ningún tipo de reglas y la información se vería expuesta a perderse en caso de un daño en el equipo donde se almacena esta información.

Tabla 29: Hallazgo 11 HC (Continuación)

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_11

PROCESO AUDITADO	CONTRATACIÓN TI		**PÁGINA**		
			2	DE	2
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de Datos (DS11)		

RIESGO:

- **Probabilidad de ocurrencia:** 64.7%
- **Impacto según relevancia del proceso**: Medio

RECOMENDACIONES:

- Incluir dentro de las políticas para la realización de las copias de seguridad:

  - Realización diaria de copias de seguridad de la información que se actualiza frecuentemente.
  - Realización semanal de copias de seguridad de la información menos sensible.
  - Conservar al menos una semana la copia de seguridad diaria.
  - Conservar al menos un mes la copia de seguridad semanal.
  - Conservar una copia de cada mes al menos durante un año.
  - Conservar una copia anual de toda la información.

- Elaborar políticas y/o procedimientos sobre los periodos de retención y los términos de almacenamiento de la información.

- Desarrollar políticas y/o procedimientos para garantizar la seguridad de la información sensible durante el transporte de la misma.

- Buscar un lugar ubicado fuera de las instalaciones del hospital, donde se pueda guardar de forma segura las copias de seguridad.

Tabla 30: Hallazgo 12 HC

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_12

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA**	
				1	DE 3
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de las instalaciones (DS12)		

DESCRIPCIÓN:

- No existe dentro de las políticas de seguridad para controlar el acceso a las instalaciones:

  - Registro de los equipos de computo (portátiles, PC, etc.) que ingresan a las instalaciones.
  - Para los visitantes que ingresan por el parqueadero de vehículos y motocicletas, se realiza la identificación, autenticación y autorización para el ingreso.
  - Se realizan requisas de los usuarios de los vehículos que ingresan y salen de las instalaciones.

- No existen controles para restringir el acceso físico de las personas Hospital Civil de Ipiales.

- No existe en las instalaciones un espacio reservado y adecuado para los equipos de cómputo que soportan el proceso de contratación TI.

- El lugar donde actualmente se encuentran instalados los equipos de cómputo claves (servidores, routers, switchs, etc.) es inadecuado.

  REF: CCUAN_HC_DS12/preguntas: 2, 3, 4, 5.

Tabla 30: Hallazgo 12 HC (Continuación)

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_12

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA**	
				2 DE 3	
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de las instalaciones (DS12)		

C**ONSECUENCIAS:**

- Las pocas medidas de seguridad que actualmente se evidencian en lo referente al acceso y salida de las instalaciones de la entidad, no brindan ningún tipo de seguridad para los activos de TI, se pueden presentar robos de elementos de tipo hardware (monitores, torres, discos duros, etc.).

- La no existencia de un centro de computo que cumpla con las características de espacio y movilidad, iluminación, tratamiento acústico, sistemas de ventilación seguridad física y suministro eléctrico, puede ocasionar daños graves en los equipos en algunos casos de pérdida total.

RIESGO:

- **Probabilidad de ocurrencia:** 79%
- **Impacto según relevancia del proceso:** Bajo

Tabla 30: Hallazgo 12 HC (Continuación)

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF** **HHC_12**

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA** 3 DE 3	
RESPONSABLE	LUIS CARLOS CHAVES YELA RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de las instalaciones (DS12)		

RECOMENDACIONES:

- Se debe establecer dentro de las políticas de seguridad para controlar el acceso a las instalaciones:

  - Registro de los equipos de computo (portátiles, PC, etc.) que ingresan a las instalaciones.
  - Para los visitantes que ingresan por el parqueadero de vehículos y motocicletas, se realiza la identificación, autenticación y autorización para el ingreso.
  - Se realizan requisas de los usuarios de los vehículos que ingresan y salen de las instalaciones.

- Establecer controles para restringir el acceso físico de las personas Hospital Civil de Ipiales.

- Preparar un espacio adecuado para los equipos de cómputo que soportan el proceso de contratación TI.

- Construir o adecuar un lugar para ubicar los equipos de cómputo claves (servidores, routers, switchs, etc.) de la entidad, este lugar debe contar con las siguientes características:

  - Espacio y movilidad.
  - Iluminación
  - Tratamiento acústico.
  - Sistemas de ventilación.
  - Seguridad física.
  - Suministro electrónico

Tabla 31: Hallazgo 13 HC

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_13

PROCESO AUDITADO	CONTRATACIÓN TI		**PÁGINA**		
			1	DE	1
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de la operación (DS13)		

DESCRIPCIÓN:

- No existen estrategias que garanticen el adecuado mantenimiento de la infraestructura que maneja el proceso contratación TI.

  REF: CCUAN_HC_DS13/preguntas: 3, 4, 5.

CONSECUENCIAS:

- Sin estas estrategias el proceso de contratación TI podría fallar en cualquier momento si se presenta una eventualidad que no se pueda controlar.

RIESGO:

- Probabilidad de ocurrencia: 60%
- Impacto según relevancia del proceso: Bajo.

RECOMENDACIONES:

- Elaborar estrategias que garanticen el adecuado mantenimiento de la infraestructura que maneja el proceso contratación TI, documentarlas y darlas a conocer a los empleados de la entidad.

Tabla 32: Hallazgo 14 HC

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_14

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA**	
				1 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Monitorear y evaluar	**PROCESO**	Monitorear y Evaluar el Control Interno (ME2)		

DESCRIPCIÓN:

- No existen políticas y procedimientos referentes al monitoreo de las actividades encaminadas a brindar seguridad física y lógica a los activos de Tecnologías de la Información del SICE y SECOP.

  REF: CCUAN_HC_ME2/preguntas: 1, 2, 3, 4.

CONSECUENCIAS:

- La no existencia de políticas y/o procedimientos para realizar el monitoreo de las actividades encaminadas a brindar seguridad física y lógica para los activos de Tecnologías de la Información del Sistema Integral de Información, hace imposible la identificación de las falencias que con respecto a estos procesos se presentan en la entidad.

RIESGO:

- Probabilidad de ocurrencia: 100%
- Impacto según relevancia del proceso: medio

Tabla 32: Hallazgo 14 HC (Continuación)

	HALLAZGO HOSPITAL CIVIL DE IPIALES E.S.E	**REF**
		HHC_14

PROCESO AUDITADO	CONTRATACIÓN TI			**PÁGINA**	
				2 DE 2	
RESPONSABLE	LUIS CARLOS CHAVES YELA				
	RICARDO ALEXANDER CABRERA SOLARTE				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Monitorear y evaluar	**PROCESO**	Monitorear y Evaluar el Control Interno (ME2)		

RECOMENDACIONES:

- Realizar un documento de políticas y procedimientos referentes al monitoreo de las actividades encaminadas a brindar seguridad física y lógica a los activos de Tecnologías de la Información del SICE y SECOP, donde se observe:

  - Descripción detallada de los procedimientos de monitoreo que se deben aplicar.
  - La periodicidad ideal para efectuar los procesos de monitoreo.
  - ¿Quién debe ejecutar el monitoreo?

3.2.4. Informe de Auditoria

- **Objetivos.** Realizar Auditoria de Sistemas a las entidades públicas Hospital Universitario Departamental de Nariño E.S.E y Hospital Civil de Ipiales E.S.E para evidenciar vulnerabilidades de seguridad física y lógica a las que se encuentra expuesta la información manejada en el proceso de contratación.

- **Objetivos Específicos**

  - ✓ Analizar y evaluar políticas de control de riesgos dentro de las entidades.

  - ✓ Analizar las políticas existentes en las entidades que garantizan la seguridad física y lógica de la información.

  - ✓ Establecer el estado de las políticas que garantizan la continuidad en el proceso de contratación de las entidades.

  - ✓ Analizar el proceso de contratación de las entidades así como las vulnerabilidades a las que este se encuentra expuesto.

  - ✓ Aportar información que permita a las entidades auditadas implementar las medidas necesarias, para garantizar que los tramites realizados por sus usuarios tengan como materia prima información confiable, integra y confidencial, que asegure la trasparencia en los procesos.

  - ✓ Analizar las instalaciones físicas que las entidades poseen, que garantizan la seguridad de la información.

- **Limitaciones.** La auditoria se realizo con completa normalidad, sin embargo cabe resaltar que en ningún momento se tuvo acceso a códigos fuentes, servidores en funcionamiento, ni módulos de aplicaciones.

- **Resultados de la Auditoría**

  - ✓ **Hospital Universitario Departamental de Nariño E.S.E.** A continuación se presentan los resultados de la auditoría aplicada al proceso Contratación TI del Hospital Universitario Departamental de Nariño, también se presentan las recomendaciones de mejoramiento para cada uno de los procesos COBIT auditados.

    - o **DOMINIO - PLANIFICACION Y ORGANIZACIÓN (PO)**

      - ▪ **Proceso COBIT PO2: Definición de la Arquitectura de la Información**

Observaciones

- El manual de políticas de seguridad existe pero se encuentra desactualizado y no ha sido dado a conocer a los empleados de la entidad.

  (REF: HHD_01)

Recomendaciones

- Actualizar periódicamente el manual de políticas de seguridad de la información.

- Aplicar los cambios que se crean convenientes al manual de políticas de seguridad de la información.

- Dar a conocer a la planta de personal el manual de políticas de seguridad de la información.

- **Proceso COBIT PO4: Definición de la Organización y las Relaciones de TI.**

Observaciones

- No existe manual de funciones para los trabajadores que interactúan con SICE y SECOP

- No existe planes de reemplazo para funcionarios en caso de ausencia

- No existen políticas adecuadas para la contratación de personal que se involucre con tecnologías de la información

- No se aplican los principios de meritocracia en la entidad

  (REF: HHD_02)

Recomendaciones

- Se recomienda crear el manual de funciones para los encargados de los sistemas SICE y SECOP

- Se debe eliminar la dependencia hacia los funcionarios por lo tanto cada proceso critico y su información debe ser soportado por al menos dos funcionarios del mismo nivel

- Se debe crear una política completamente clara acerca del proceso contratación TI esto eliminara cualquier manto de duda, esto le dará a la entidad la transparencia que requiere

- **Proceso COBIT PO7: Administración de recursos humanos**

  Observaciones

  - No existen políticas ni procedimientos claros para realizar el proceso contratación TI

  - No todas las personas que cumplan con los lineamientos del cargo pueden aspirar a él.

  - No se aplican procesos de selección transparentes ante la sociedad

    (REF: HHD_03)

  Recomendaciones

  - Crear una política para contratación TI clara, con procesos transparentes y con lineamientos que permitan claridad y transparencia hacia la sociedad en general.

- **Proceso COBIT PO9: Evaluación de Riesgos**

  Observaciones

  - Los sistemas SICE y SECOP se encuentran totalmente expuestos a fallas por que no existen políticas ni procedimientos para la evaluación de riesgos

  - Al momento de realizar cambios en los procedimientos no se tienen en cuenta a los empleados que manejan estos procedimientos

  - La entidad no cuenta con un procedimiento claro para el acoplamiento en los cambios externos gubernamentales

  - No existe un record de incidentes o inspecciones que den una alternativa para la resolución de conflictos

  - No hay un ranking o categorización de riesgos

    (REF: HHD_04)

Recomendaciones

- Se recomienda tener en cuenta los requerimientos externos de cambio sin importar de que tipo sean

- Se debe crear una categorización clara de riesgos para su control y evaluación y posteriormente hacer un archivo de los mismos para su consulta que permita la oportuna resolución de riesgos

o **DOMINIO - ADQUISICION E IMPLEMENTACION (AI)**

- **Proceso COBIT AI2: Adquisición y mantenimiento del software aplicativo.**

  Observaciones

  - En la entidad no existe un plan de depuración de datos

  - En la entidad no existe un manual para el manejo de los sistemas SICE y SECOP

    (REF: HHD_05)

  Recomendaciones

  - Se debe crear y poner en marcha un plan de depuración de datos

  - Se debe crear y poner en marcha un manual adecuado para el manejo de los sistemas SICE y SECOP

- **Proceso COBIT AI3: Adquisición y Mantenimiento de la Infraestructura Tecnológica**

  Observaciones

  - Las políticas y procedimientos para la adquisición de hardware no se encuentran bien fundamentadas.

  - Las políticas y procedimientos para la adquisición de hardware no se encuentran documentadas

  - Las políticas y procedimientos para la adquisición de hardware no son conocidas por los funcionarios

- Los procedimientos para el mantenimiento preventivo de los equipos de la entidad no son los mejores ni los mas óptimos

- Las políticas y procedimientos de mantenimiento preventivo de los equipos de la entidad no se encuentra documentada por completo

- Las políticas y procedimientos de mantenimiento preventivo de los equipos de la entidad no son de conocimiento de toda la planta de funcionarios

- Las reparaciones son llevadas a cabo por los mismos funcionarios sin importar de que tipo sean

- Las políticas y procedimientos para la adquisición de software no se encuentran bien fundamentadas.

- Las políticas y procedimientos para la adquisición de software no se encuentran documentadas

- Las políticas y procedimientos para la adquisición de software no son conocidas por los funcionarios

  (REF: HHD_06)

Recomendaciones

- Al no existir políticas de adquisición de hardware se puede incurrir en gastos redundantes, que derivan en el detrimento del patrimonio público al ser una entidad regulada por el estado.

- Al no existir políticas de adquisición de software se puede incurrir en gastos redundantes, que derivan en el detrimento del patrimonio público al ser una entidad regulada por el estado

- Al no existir buenas políticas para el mantenimiento preventivo de los equipos, este podría quedar mal hecho lo que generaría gastos posteriores

- Ya que los encargados de los arreglos a los equipos no son las personas mas idóneas, estos arreglos pueden causar un daño mucho más grave en estos equipos lo que generaría gastos mayores

- **DOMINIO - ENTREGAR Y DAR SOPORTE (DS)**

  - **Proceso COBIT DS4: Asegurar Continuidad de Servicios**

Observaciones

- Existen estrategias para garantizar el proceso contratación TI pero estas no son las mas optimas ni se encuentran actualizadas

- No existe un plan adecuado para la recuperación ante desastres

- No se ha programado un plan para la distribución de la documentación de los planes de riesgo

- En el plan de continuidad no se contempla el impacto al proceso contratación TI

- Los funcionarios no conocen las estrategias de actuación frente a un desastre

- La información se encuentra centralizada lo que genera un caos de datos si se presentara una pérdida

  (REF: HHD_07)

Recomendaciones

- Crear un plan de recuperación de datos en caso de desastres

- Dar a conocer el plan de recuperación de datos en caso de desastres a todo el personal de la entidad

- Descentralizar la información

- **Proceso DS5: Garantizar la Seguridad de los Sistemas**

Observaciones

- Existe una política de seguridad lógica en la entidad pero esta no está bien fundamentada ni actualizada

- Existen políticas control de acceso pero no se encuentran actualizadas ni están correctamente diseñadas

- Las políticas de control de acceso no son del todo conocidas, ni puestas en práctica por los funcionarios de la entidad

- El software que defiende las terminales de ataques de virus, troyanos, gusanos y demás no se encuentra actualizado correctamente y en algunos casos carece de licencia

  (REF: HHD_08)

Recomendaciones

- Crear y poner en marcha una política clara y contundente de seguridad lógica

- Actualizar y licenciar según sea el caso el software que defiende las terminales de trabajo de la entidad

- **Proceso COBIT DS9: Administración de la Configuración**

Observaciones

- No hay claridad en las políticas respecto al software que la entidad permite instalar en sus terminales

- No hay políticas procedimientos claros respecto a hardware permitido por la entidad

- No hay documentación de las políticas que regulan la instalación o utilización de hardware y software

- No hay controles hacia los funcionarios que podrían utilizar software y hardware desconocido

  (REF: HHD_09)

Recomendaciones

- Crear y poner en marcha una política clara con respecto al software y hardware que los funcionarios pueden instalar y manipular en los equipos de la entidad

- Realizar los controles necesarios y regulares hacia los funcionarios y equipos con respecto a hardware y software que puede o no ser utilizado e instalado en la entidad

- **Proceso COBIT DS10: Administración de Problemas**

Observaciones

- No hay estrategias que permitan identificar y rastrear posibles riesgos en el proceso contratación TI.

  (REF: HHD_10)

Recomendaciones

- Crear estrategias que permitan identificar y rastrear posibles riesgos en el proceso contratación TI

- **Proceso COBIT DS11: Administración de Datos**

Observaciones

- No existe la documentación de las políticas de copias de seguridad de la información

- No se encuentran definidos los procedimientos para los periodos de retención y los términos de almacenamiento de la información

- La información es almacenada en el archivo central de la entidad, y descansa solo en ese lugar lo que acarrea problemas ante posibles desastres o filtraciones de información.

  (REF: HHD_11)

Recomendaciones

- Crear la documentación de las políticas de copias de seguridad

- Crear un plan de archivo exterior con todas las políticas y procedimientos que esto implica

- **Proceso COBIT DS12: Administración de las Instalaciones**

Observaciones

- Las políticas de seguridad para el ingreso a la entidad se encuentran bien fundamentadas pero existen algunas fallas cuando el ingreso se hace por medio de algún vehículo

- La entidad no cuenta con un centro de cómputo adecuado, y no posee la seguridad necesaria.

- En el lugar donde se están llevando a cabo las tareas de centro de cómputo no se cuentan con las condiciones adecuadas de espacio, iluminación, ventilación, seguridad física y demás necesarias para un buen funcionamiento.

  (REF: HHD_12)

Recomendaciones

- Se recomienda extender las políticas de seguridad para el ingreso a la entidad, y acrecentarlas cuando se trata de vehículos automotores

- Se recomienda crear un centro de cómputo con las condiciones necesarias para asegurar las condiciones de trabajo y de los procesos

- **Proceso COBIT DS13: Administración de la operación**

Observaciones

- No existen estrategias que garanticen el adecuado resguardo de la información

- No existe un adecuado inventario de estos resguardos de información.

  (REF: HHD_13)

Recomendaciones

- Se debe crear y poner en marcha las estrategias que garanticen el resguardo de la información sensible para el proceso

- Se debe crear un adecuado resguardo para la información sensible del proceso

- Se debe crear una estrategia que garantice el adecuado mantenimiento de la infraestructura que maneja el proceso contratación TI

- **DOMINIO - MONITOREAR Y EVALUAR (ME)**

  - **Proceso COBIT M2: Evaluar lo Adecuado del Control Interno**

Observaciones

- No existe un monitoreo constante de actividades dentro del proceso contratación TI, que pretendan brindar mayor seguridad física y lógica a los activos físicos o de información que soportan el mencionado proceso.

  (REF: HHD_14)

Recomendaciones

- Crear las políticas de monitoreo que permitan brindar mayor seguridad física y lógica a los activos de tecnología de la información de los sistemas SICE y SECOP

- **Resultados de la Auditoría**:

  - ✓ **Hospital Civil de Ipiales E.S.E.** A continuación se presentan los resultados de la auditoría aplicada al proceso Contratación TI del Hospital Civil de Ipiales, también se presentan las recomendaciones de mejoramiento para cada uno de los procesos COBIT auditado.

    - o **DOMINIO - PLANIFICACION Y ORGANIZACIÓN (PO)**

      - **Proceso COBIT PO2: Definición de la Arquitectura de la Información**

        Observaciones

        - No existe un procedimiento establecido para mantener actualizado el Manual de Políticas de seguridad de la información.

          (REF: HHC_01)

        Recomendaciones

        - Establecer un proceso para mantenerlo actualizado el Manual de Políticas de seguridad de la información.

      - **Proceso COBIT PO4: Definición de la Organización y las Relaciones de TI.**

        Observaciones

        - No existe un manual de funciones para los empleados que interactúan con el SICE y SECOP, además de un procedimiento para realizar la contratación del personal que se involucre con tecnologías de información.

          (REF: HHC_02)

        Recomendaciones

        - Realizar un manual de funciones para los empleados que interactúan con el SICE y SECOP donde se especifique

        - Una identificación clara de los roles o cargos que los funcionarios deberán desempeñar.

- Las responsabilidades y roles para los funcionarios que interactúan con estos sistemas.

- Las funciones que los funcionarios deben desempeñar de acuerdo con los roles y responsabilidades que se les fue asignado.

- La descripción de los perfiles que deben poseer los funcionarios que interactúan con los estos sistemas.

- La descripción de los procesos que los usuarios de los sistemas SICE y SECOP deben seguir para garantizar la seguridad de la información.

- **Proceso COBIT PO7: Administración de recursos humanos**

  Observaciones

  - No existe un manual de funciones para los empleados que interactúan con el SICE y SECOP, además de un procedimiento para realizar la contratación del personal que se involucre con tecnologías de información.

    (REF: HHC_03)

  Recomendaciones

  - Elaborar un documento donde se describan las políticas y procedimientos para realizar la contratación del personal que se involucre con tecnologías de información.

- **Proceso COBIT PO9: Evaluación de Riesgos**

  Observaciones

  - No existe un marco referencial y procedimientos para la evaluación de riesgos, además de un plan de acción contra riesgos.

    (REF: HHC_04)

  Recomendaciones

  - Desarrollar un marco referencial y procedimientos para la evaluación de riesgos, donde se especifique:

- Aspectos relacionados con la actualización o mantenimiento del hardware e infraestructura de red.

- Cambios en los requerimientos de los usuarios.

- Cambios en los requerimientos externos gubernamentales.

- Auditorias, inspecciones, o incidentes anteriores ocurridos en relación a las tecnologías de información del Hospital.

- Elaborar un plan de acción contra riesgos y establecer políticas o procedimientos para la adquisición de pólizas de seguros para el manejo de los riesgos.

o **DOMINIO - ADQUISICION E IMPLEMENTACION (AI)**

▪ **Proceso COBIT AI2: Adquisición y mantenimiento del software aplicativo.**

Observaciones

- No existe un manual para el manejo de SECOP y SICE.

- No existe algún plan de depuración de datos.

(REF: HHC_05)

Recomendaciones

- Elaborar un manual para el manejo de SECOP y SICE y un plan de depuración de datos.

- Elaborar un plan de depuración de datos.

▪ **Proceso COBIT AI3: Adquisición y Mantenimiento de la Infraestructura Tecnológica**

Observaciones

- No existen políticas y procedimientos para la adquisición de hardware aunque se tiene en cuenta la opinión de un experto en el equipo que se va a adquirir.

- No existen políticas y procedimientos para la adquisición de software aunque se realiza un proceso adecuado a la hora de adquirirlo.

- No existen políticas para llevar a cabo el mantenimiento preventivo o correctivo de los equipos de cómputo.

  (REF: HHC_06)

Recomendaciones

- Desarrollar políticas y procedimientos para la adquisición de hardware donde se especifiquen:

- La realización de una solicitud de compra formal y por escrito del hardware

- La solicitud describe las características que debe poseer el hardware

- La solicitud describe la necesidad de adquisición del hardware

- La cotización de diferentes proveedores del hardware a comprar

- Análisis de las propuestas de los proveedores

- Se elige la propuesta de adquisición de hardware más favorable para la entidad.

- Desarrollar políticas y procedimientos para la adquisición de software donde se especifiquen:

- La realización de una solicitud de compra formal y por escrito del software

- La solicitud describe las características que debe poseer el software

- La solicitud describe la necesidad de adquisición del software

- La realización del proceso de análisis para determinar si se compra software comercial o se contrata la realización de software a la medida

- El software comercial que se adquiera deberá ser legal y contar con su respectiva licencia.

- Si se contrata el desarrollo se contempla información sobre la plataforma en la que sea desarrollado el software.

- Elaborar políticas para llevar a cabo el mantenimiento preventivo o correctivo de los equipos de cómputo

o **DOMINIO - ENTREGAR Y DAR SOPORTE (DS)**

- **Proceso COBIT DS4: Asegurar Continuidad de Servicios**

Observaciones

- En el manual de contratación no se tiene en cuenta planes de recuperación ante desastres, definición del esquema de análisis de riesgo, documentación y distribución de los planes de riesgo.

- No existe un plan de continuidad que contemple la identificación de los procesos críticos y el análisis de impacto.

(REF: HHC_07)

Recomendaciones

- Incluir dentro del manual de contratación:

- Planes de recuperación ante desastres

- Definición del esquema de análisis de riesgo

- Documentación y distribución de los planes de riesgo.

- Elaborar un plan de continuidad que contemple la identificación de los procesos críticos y el análisis de impacto donde se especifique:

- Guía de cómo utilizar el plan

- Procedimientos de evacuación del personal

- Tipos de condiciones para ser declarado un desastre

- Identificación de los elementos críticos que deben ser recuperados tras un desastre

- Explicación de los procedimientos de emergencia que se deben realizar en caso de desastre.

- **Proceso COBIT DS5: Garantizar la Seguridad de los Sistemas**

Observaciones

- Dentro de las políticas de seguridad lógica en la entidad no se tiene en cuenta:
- Reportes y revisión de las violaciones e incidentes de seguridad
- Administración de llaves criptográficas
- Detección, resolución y comunicación sobre los virus
- Clasificación y propiedad de los datos
- No existen políticas de control de contraseñas.

  (REF: HHC_08)

Recomendaciones

- Incluir dentro de las políticas de seguridad lógica en la entidad:
- Reportes y revisión de las violaciones e incidentes de seguridad
- Administración de llaves criptográficas
- Detección, resolución y comunicación sobre los virus
- Clasificación y propiedad de los datos.
- Elaborar políticas de control de contraseñas donde se especifique:
- Cambio periódico de contraseña
- Longitud adecuada de contraseña
- Combinaciones alfanuméricas obligatorias
- Protección de las contraseñas

▪ **Proceso COBIT DS9: Administración de la Configuración**

Observaciones

- No existe un inventario de la configuración de las terminales de trabajo de los usuarios que interactúan con el SICE y SECOP.

  (REF: HHC_09)

Recomendaciones

- Desarrollar un inventario de la configuración de las terminales de trabajo de los usuarios que interactúan con el SICE y SECOP donde se observe claramente:

- La configuración referente al Sistema Operativo de las terminales

- La configuración del software instalado en las diferentes terminales

- Información referente a las licencias de los diferentes programas instalados en las terminales de trabajo

- La configuración del hardware instalado.

- **Proceso COBIT DS10: Administración de Problemas**

Observaciones

- No existen estrategias que garanticen el rastreo de problemas en el proceso contratación TI.

  (REF: HHC_10)

Recomendaciones

- Establecer estrategias que garanticen el rastreo de problemas en el proceso contratación TI donde se describa:

- Planes de recuperación

- Definición del esquema de análisis de riesgo

- Documentación y distribución de los planes de riesgo

- Resolución de problemas rastreados

- **Proceso COBIT DS11: Administración de Datos**

Observaciones

- En las políticas para la realización de las copias de seguridad no se tiene en cuenta:

- Realización diaria de copias de seguridad de la información que se actualiza frecuentemente.

- Realización semanal de copias de seguridad de la información menos sensible

- Conservar al menos una semana la copia de seguridad diaria

- Conservar al menos un mes la copia de seguridad semanal

- Conservar una copia de cada mes al menos durante un año

- Conservar una copia anual de toda la información.

(REF: HHC_11)

Recomendaciones

- Incluir dentro de las políticas para la realización de las copias de seguridad:

- Realización diaria de copias de seguridad de la información que se actualiza frecuentemente.

- Realización semanal de copias de seguridad de la información menos sensible

- Conservar al menos una semana la copia de seguridad diaria

- Conservar al menos un mes la copia de seguridad semanal

- Conservar una copia de cada mes al menos durante un año

- Conservar una copia anual de toda la información.

- Elaborar políticas y/o procedimientos sobre los periodos de retención y los términos de almacenamiento de la información.

- Desarrollar políticas y/o procedimientos para garantizar la seguridad de la información sensible durante el transporte de la misma.

- Buscar un lugar ubicado fuera de las instalaciones del hospital, donde se pueda guardar de forma segura las copias de seguridad.

- **Proceso COBIT DS12: Administración de las Instalaciones**

Observaciones

- No existe dentro de las políticas de seguridad para controlar el acceso a las instalaciones:

- Registro de los equipos de computo (portátiles, PC, etc.) que ingresan a las instalaciones.

- Para los visitantes que ingresan por el parqueadero de vehículos y motocicletas, se realiza la identificación, autenticación y autorización para el ingreso

- Se realizan requisas de los usuarios de los vehículos que ingresan y salen de las instalaciones.

- No existen controles para restringir el acceso físico de las personas Hospital Civil de Ipiales.

- No existe en las instalaciones un espacio reservado y adecuado para los equipos de cómputo que soportan el proceso de contratación TI.

- El lugar donde actualmente se encuentran instalados los equipos de cómputo claves (servidores, routers, switchs, etc.) es inadecuado.

(REF: HHC_12)

Recomendaciones

- Se debe establecer dentro de las políticas de seguridad para controlar el acceso a las instalaciones

- Registro de los equipos de computo (portátiles, PC, etc.) que ingresan a las instalaciones.

- Para los visitantes que ingresan por el parqueadero de vehículos y motocicletas, se realiza la identificación, autenticación y autorización para el ingreso.

- Se realizan requisas de los usuarios de los vehículos que ingresan y salen de las instalaciones:

- Establecer controles para restringir el acceso físico de las personas Hospital Civil de Ipiales.

- Preparar un espacio adecuado para los equipos de cómputo que soportan el proceso de contratación TI.

- Construir o adecuar un lugar para ubicar los equipos de cómputo claves (servidores, routers, switchs, etc.) de la entidad, este lugar debe contar con las siguientes características:

  - Espacio y movilidad.

  - Iluminación

  - Tratamiento acústico.

  - Sistemas de ventilación.

  - Seguridad física.

  - Suministro electrónico

- **Proceso COBIT DS13: Administración de la operación**

  Observaciones

  - No existen estrategias que garanticen el adecuado mantenimiento de la infraestructura que maneja el proceso contratación TI.

    (REF: HHC_13)

  Recomendaciones

  - Elaborar estrategias que garanticen el adecuado mantenimiento de la infraestructura que maneja el proceso contratación TI, documentarlas y darlas a conocer a los empleados de la entidad.

- **DOMINIO - MONITOREAR Y EVALUAR (ME)**

  - **Proceso COBIT M2: Evaluar lo Adecuado del Control Interno**

    Observaciones

- No existen políticas y procedimientos referentes al monitoreo de las actividades encaminadas a brindar seguridad física y lógica a los activos de Tecnologías de la Información del SICE y SECOP.

  (REF: HHC_14)

Recomendaciones

- Realizar un documento de políticas y procedimientos referentes al monitoreo de las actividades encaminadas a brindar seguridad física y lógica a los activos de Tecnologías de la Información del SICE y SECOP, donde se observe:

- Descripción detallada de los procedimientos de monitoreo que se deben aplicar.

- La periodicidad ideal para efectuar los procesos de monitoreo.

- ¿Quién debe ejecutar el monitoreo?

- **Evaluación de la usabilidad y del decreto 1151 de 2008 de Gobierno en Línea.**

  ✓ **Hospital Universitario Departamental de Nariño Decreto 1151 de 2008 de Gobierno en Línea**

Tabla 33: GL - HD

Nombre de la entidad	Hospital Universitario Departamental de Nariño E.S.E
Municipio	Pasto
Nit	891200528-8
Dirección	Calle 22 Nº 7 – 93 Parque Bolívar
Teléfono	7319568
Correo Electrónico	departamental@hosdenar.gov.co

1. La Entidad cuenta con un sitio Web?	
X	SI
	NO
	En desarrollo
2. Si cuenta con un sitio web, o está en desarrollo escriba la dirección.	
	http://www.hosdenar.gov.co
3. La entidad cuenta con un Comité de Gobierno en línea? Si la respuesta es positiva indicar el acto administrativo y fecha de expedición.	
	SI ACTO ADMINISTRATIVO _____
X	NO
4. Si la respuesta fue SI, relacione los cargos de los integrantes del Comité de Gobierno en Línea:	
	_____
	_____
	_____
	_____
	_____
	_____
5. Con que periodicidad se reúne el comité de Gobierno en línea	
	Mensualmente
	Bimensualmente
	Trimestralmente
	Semestralmente
	Otro CUAL?

Tabla 33: GL – HD (Continuación)

6. El comité realiza un seguimiento sobre la implementación de Gobierno en línea en la entidad?	
	SI
	NO
7. El comité ha realizado algún informe sobre el avance de la implementación de la estrategia del Gobierno en línea.	
	SI
	NO

Las siguientes preguntas pertenecen a la primera Fase de la estrategia (Información en línea), y deberán responderse teniendo en cuenta la inclusión o existencia de la respectiva información, en el sitio Web de la Entidad.

Marcar **SI** cuando el sitio Web contenga la información indicada.
Marcar **NO** cuando el sitio Web no tenga la información indicada.
Marcar **EN DESARROLLO** cuando el ítem respectivo se encuentre en elaboración.

Tabla 34: GL2 - HD

1. Acerca de la Entidad	**SI**	**NO**	**EN DESARROLLO**
a. Misión y visión		X	
b. Objetivos y funciones	X		
c. Organigrama		X	
d. Localización física (incluyendo todas las sedes o sucursales)	X		
e. Teléfonos y/o líneas gratuitas y fax	X		
f. Correo electrónico de contacto		X	
g. Horarios y días de atención al público		X	
h. Directorio de funcionarios principales		X	
i. Directorio de entidades		X	
j. Directorio de agremiaciones y asociaciones	X		
2. Leyes y normatividad vigentes	**SI**	**NO**	**EN DESARROLLO**
a. Leyes/ Ordenanzas /Acuerdos	X		
b. Decretos	X		

Tabla 34: GL2 – HD (Continuación)

c. Resoluciones y/u otros actos administrativos de carácter general		X	
d. Proyectos de normatividad		X	
3. Presupuesto	**SI**	**NO**	**EN DESARROLLO**
a. Presupuesto aprobado en ejercicio de acuerdo con las normas vigentes	X		
b. Información histórica de presupuestos		X	
4. Políticas, planes, programas y proyectos institucionales	**SI**	**NO**	**EN DESARROLLO**
a. Políticas, planes y/o líneas estratégicas	X		
b. Programas y proyectos en ejecución		X	
c. Contacto con dependencia responsable		X	
5. Contratación	**SI**	**NO**	**EN DESARROLLO**
a. Información sobre Licitaciones, selecciones abreviadas, concurso de mérito y Contratación Directa	X		
b. Información sobre Contratos en Ejecución		X	
6. Control y rendición de cuentas	**SI**	**NO**	**EN DESARROLLO**
a. Entes de control que vigilan a la Entidad			X
b. Informes de gestión	X		
c. Metas, indicadores de gestión y/o desempeño y resultados		X	
d. Plan de mejoramiento		X	
7. Servicios de información	**SI**	**NO**	**EN DESARROLLO**
a. Información para niños		X	
b. Preguntas y respuestas frecuentes		X	
c. Boletines y publicaciones	X		
d. Noticias			X

Tabla 34: GL2 – HD (Continuación)

e. Calendario de actividades		X	
f. Glosario		X	
g. Política de privacidad y condiciones de uso		X	
8, Estándares de Presentación	**SI**	**NO**	**EN DESARROLLO**
a. Identidad visual (escudo de la República e identidad visual de la Entidad)		X	
b. Enlace al Portal del Estado Colombiano www.gobiernoenlinea.gov.co			X
c. Fecha de la última actualización del sitio Web	X		
d. División de los contenidos (divididos en porciones pequeñas)	X		
e. Uso de colores (pocos colores, sin caer en un diseño monótono)	X		
f. Manejo de vínculos (textos que indiquen claramente al usuario el contenido de la página Web)	X		
9. Estándares de Funcionalidad	**SI**	**NO**	**EN DESARROLLO**
a. Mapa del sitio		X	
b. Acceso a la página de inicio	X		
c. Acceso al menú principal	X		
10. Estándares Técnicos	**SI**	**NO**	**EN DESARROLLO**
a. Nombre del dominio con formato www.nombredelaentidad.gov.co, .edu.co ó .mil.com	X		
b. Tiempo de despliegue de una página en el navegador de usuario no mayor a 20 segundos	X		
c. Elementos como gráficos o archivos sonoros marcados y/o etiquetados con una descripción de su contenido			X
d. Elementos gráficos que se muevan, parpadeen se desplacen o se actualicen automáticamente con la posibilidad de ser detenidos temporal o totalmente.		X	

✓ **Usabilidad**

Tabla 35: Usabilidad – HD

Institución:	***Hospital Universitario Departamental de Nariño E.S.E***			
Url:	http://www.hosdenar.gov.co			
Evaluador:	***Luis Carlos Chaves Yela - Ricardo Cabrera Solarte***			
Fecha:	***19/06/2010***			
Nota:	***6,4***			
20%		**1. Usabilidad**	**6,7**	**1,3**
	40%	**1.1 Comprensibilidad Global del Sitio**	**5,0**	**2,0**
		1.1.1 Esquema de Organización Global	**3,0**	
		1.1.1.1 Mapa del Sitio	1	
		1.1.1.2 Índice Global (por Temas, etc.)	7	
		1.1.1.3 Tabla de Contenidos	1	
		1.1.2 Calidad en el Sistema de Etiquetado	**9,0**	
		1.1.2.1 Etiquetado Textual	9	
		1.1.2.2 Etiquetado con Iconos	9	
		1.1.3 Visita Guiada	**1,0**	
		1.1.3.1 Visita Convencional	1	
		1.1.3.2 Visita Virtual (con Tecnología VR)	1	
		1.1.4 Página Principal	**7,2**	
		1.1.4.1 Navegabilidad de la página principal	7	
		1.1.4.2 Impacto de la página principal	8	
		1.1.4.2.1 La página principal refleja la idea del sitio	9	
		1.1.4.2.2 La página principal deja claro que puedo hacer en el sitio	6	
		1.1.4.2.3 La página principal se ve bien al deshabilitar las imágenes	6	
		1.1.5 Consistencia de la navegación	**5,0**	
	10%	**1.2 Mecanismos de Ayuda y Retroalimentación en línea**	**2,8**	**0,3**
		1.2.1 Calidad de la Ayuda	**1,0**	
		1.2.1.1 Ayuda Explicatoria acerca del sitio	1	
		1.2.1.2 Ayuda de la Búsqueda	1	
		1.2.2 Indicador de Ultima Actualización	**1,0**	
		1.2.2.1 Global (de todo el sitio Web)	1	
		1.2.2.2 Restringido (subsitio o página)	1	
		1.2.2.3 Por noticias (Solo ultimas noticias)	1	
		1.2.3 Directorio de Enlaces	**8,0**	
		1.2.3.1 Enlaces a sitios de Interés	8	
		1.2.3.2 Enlaces a asociaciones de interés	8	
		1.2.4 Facilidad FAQ	**1,0**	

Tabla 35: Usabilidad – HD (Continuación)

	10%	**1.3 Aspectos de Interfaces y Estéticos**	**8,1**	**0,8**
		1.3.1 Cohesividad al Agrupar los Objetos de Control Principales	**8,0**	
		1.3.2 Permanencia y Estabilidad en la Presentación de los Controles Principales	**8,5**	
		1.3.2.1 Permanencia de Controles Directos	8	
		1.3.2.2 Permanencia de Controles Indirectos	9	
		1.3.2.3 Estabilidad	9	
		1.3.3 Preferencia Estética	**9,0**	
		1.3.4 Uniformidad en el Estilo del sitio	**7,0**	
	10%	**1.4 Misceláneas**	**6,7**	**0,7**
		1.4.1 Soporte a Lenguaje Extranjero	**1,0**	
		1.4.2 Descarga de contenidos	**9,0**	
		1.4.2.1 Descarga de contenidos a multidispositivo	8	
		1.4.2.2 Descarga de contenidos	10	
		1.4.3 Intrusión publicitaria	**10,0**	
	15%	**1.5 Usabilidad de los Textos**	**9,0**	**1,4**
		1.5.1 Textos adaptados para la Web	**9,0**	
		1.5.1.1 Textos breves	9	
		1.5.1.2 Textos escaneables	9	
		1.5.1.3 Estilo de escritura conciso	9	
	15%	**1.6 Clasificación de la información**	**8,5**	**1,3**
		1.6.1 Categorías	8,5	
		1.6.1.1 Claridad de las categorías	9	
		1.6.1.2 Cohesión de las categorías	8	
10%		**2. Accesibilidad**	**6,3**	**0,6**
	70%	**2.1 Accesibilidad para usuarios con discapacidades**	**3,0**	**2,1**
		2.1.1 Discapacidades visuales	**1,0**	
		2.1.1.1 Posibilidad de modificar el tamaño de las fuentes	1	
		2.1.1.2 Combinaciones de color (para usuarios con ceguera al color)	1	
		2.1.1.3 Markup claro para poder ser leído por un lector de pantalla	1	
		2.1.1.4 Etiquetas ALT en todas las imágenes	1	
		2.1.2 Discapacidades auditivas	**5,0**	
	20%	**2.2 Acceso a navegadores no gráficos**	**6,0**	**1,2**
	10%	**2.3 Acceso Multidispositivo**	**10,0**	**1,0**
15%		**3. Funcionalidad**	**4,4**	**0,7**
	50%	**3.1 Aspectos de Búsqueda**	**1,0**	**0,5**

Tabla 35: Usabilidad – HD (Continuación)

		3.1.1 Mecanismo de Búsqueda en el Sitio	**1,0**	
		3.1.1.1 Búsqueda Restringida (por secciones)	1	
		3.1.1.2 Búsqueda Global	1	
		3.1.2 Búsqueda siempre disponible	**1,0**	
	50%	**3.2 Aspectos de Navegación y Exploración**	**7,7**	**3,9**
		3.2.1 Navegabilidad Local (de subsitio)	**7,3**	
		3.2.1.1 Nivel de Interconexión	2	
		3.2.1.2 Orientación	9	
		3.2.1.2.1 Indicador del Camino	9	
		3.2.1.2.2 Etiqueta de la Posición Actual	9	
		3.2.2 Navegabilidad Global	**7,5**	
		3.2.2.1 Acoplamiento entre Subsitios	8	
		3.2.3 Objetos de Control Navegacional	**7,8**	
		3.2.3.1 Permanencia y Estabilidad en la Presentación de los Controles Contextuales	7	
		3.2.3.1.1 Permanencia de los Controles Contextuales	7	
		3.2.3.1.2 Estabilidad	7	
		3.2.3.2 Nivel de Desplazamiento	9	
		3.2.3.2.1 Desplazamiento Vertical	8	
		3.2.3.2.2 Desplazamiento Horizontal	9	
		3.2.4 Predicción Navegacional	**8,5**	
		3.2.4.1 Enlace con Título (enlace con texto explicatorio)	9	
		3.2.4.2 Calidad de la Frase del Enlace	8	
		3.2.5 Funciones Misceláneas y Específicas del Dominio	**7,5**	
40%		**4 Contenidos**	**6,5**	**2,6**
	20%	**4.1 Información Hospitalaria**	**7,5**	**1,5**
		4.1.1 Información sobre Servicios	**10,0**	
		4.1.2 Servicios	**8,5**	
		4.1.2.1 Planes de servicios actuales	9	
		4.1.1.2 Planes de servicios futuros	8	
		4.1.3 Información sobre las Dependencias	**5,0**	
		4.1.3.1 Información sobre los Profesionales	6	
		4.1.3.2 Horarios de los Profesionales	4	
		4.1.4 Valores de la Entidad	**7,0**	
		4.1.4.1 Misión y Visión	1	
		4.1.4.2 Reglamentos	10	
		4.1.4.3 Historia	10	
		4.1.5 Información sobre Programas Institucionales	7,0	
		4.1.5.1 Información de Prevención	6	
		4.1.5.2 Programas de Atención	7	
		4.1.5.3 Programas de Salud General	7	

Tabla 35: Usabilidad – HD (Continuación)

		4.1.5.3 Programas de Especialidades	8	
	15%	**4.2 Información sobre el equipo medico**	**4,5**	**0,7**
		4.2.1 Hojas de vida de los profesionales	**4,0**	
		4.2.1.1 Intereses Académicos	4	
		4.2.1.2 Formación	4	
		4.2.2 Areas de los profesionales	**10,0**	
		4.2.3 Información de contacto	**3,0**	
		4.2.3.1 Dirección	3	
		4.2.3.2 Teléfono	3	
		4.2.3.3 Mail	3	
		4.2.4 Buscador de profesionales	**1,0**	
	15%	**4.3 Información sobre Actividades**	**6,7**	**1,0**
		4.3.1 Actividades pasadas	**7,0**	
		4.3.2 Agenda de actividades futuras	**7,0**	
		4.3.3 Descripción del evento	**7,0**	
		4.3.4 Información del ponente	**6,0**	
		4.3.5 Memoria de actividades realizadas por la institución	**6,3**	
		4.3.5.1 Descripción del evento	9	
		4.3.5.2 Información del ponente	5	
		4.3.5.3 Material utilizado	5	
	20%	**4.4 Información sobre los Programas**	**8,3**	**1,7**
		4.4.1 Objetivos	**10,0**	
		4.4.2 Contenidos	**10,0**	
		4.4.3 Evaluación	**7,0**	
		4.4.4 Horarios	**6,0**	
	10%	**4.6 Información de contacto de la Institución**	**5,5**	**0,6**
		4.6.1 Ubicación	**1,0**	
		4.6.1.1 Como llegar (transportes, distancias, etc.)	1	
		4.6.1.2 Mapa geográfico	1	
		4.6.1.3 Mapa interno	1	
		4.6.2 Contacto con responsables / asesores	**10,0**	
		4.6.2.1 Nombre	10	
		4.6.2.2 Correo	10	
		4.6.2.3 Teléfono	10	
		4.6.2.4 Fax	10	
	10%	**4.7 Información para trabajadores nuevos**	**6,3**	**0,6**
		4.7.1 Claridad de Misión y Visión	**1,0**	
		4.7.2 Historia	**9,0**	
		4.7.3 Reglamento	**9,0**	
	10%	**4.8 Información para potenciales usuarios**	**6,7**	**0,7**
		4.8.1 Por que deben elegir este Hospital	**9,0**	
		4.8.2 Claridad de Misión y Visión	**1,0**	

Tabla 35: Usabilidad – HD (Continuación)

		4.8.3 Información geográfica	**1,0**	
		4.8.4 Información de contacto para obtener mas información	**9,0**	
		4.8.5 Historia	**9,0**	
		4.8.6 Reglamento	**9,0**	
		4.8.7 Organización	**9,0**	
7,5%		**5. Confiabilidad**	**8,7**	**0,7**
	50%	**5.1 Ausencia de Deficiencias y Errores**	**7,1**	**3,6**
		5.1.1 Errores de Enlaces	**4,7**	
		5.1.1.1 Enlaces Rotos	4	
		5.1.1.2 Enlaces Inválidos	5	
		5.1.1.3 Enlaces no Implementados	5	
		5.1.2 Errores o Deficiencias Varias	**8,7**	
		5.1.2.1 Deficiencias o cualidades ausentes debido a diferentes navegadores	9	
		5.1.2.2 Nodos Web Muertos (sin enlaces de retorno)	8	
		5.1.2.3 Nodos Destinos (inesperadamente) en Construcción	9	
		5.1.3 Enlaces externos a instituciones prestigiosas	**8,0**	
	25%	**5.2 Utilización de estándares del W3C**	**10,0**	**2,5**
		5.2.1 HTML	10	
		5.2.2 CSS	10	
	25%	**5.3 Actualización periódica de la información**	**9,0**	**2,3**
7,5%		**6. Eficiencia**	**6,9**	**0,5**
	60%	**6.1 Accesibilidad de Información**	**2,8**	**1,7**
		6.1.1 Soporte a Versión sólo Texto	**2,0**	
		6.1.2 Legibilidad al desactivar la Propiedad Imagen del Browser	**3,5**	
		6.1.2.1 Imagen con Título	2	
		6.1.2.2 Legibilidad Global	5	
	20%	**6.2 Rendimiento**	**9,0**	**1,8**
	20%	**6.3 Tiempo de descarga**	**9,0**	**1,8**

La nota del sitio web resulto tan baja por que en los siguientes ítems se noto que no cumplieron a cabalidad con las condiciones necesarias de manejo y usabilidad.

Mapa del Sitio: El mapa del sitio nunca es encontrado por el servidor, no existe la pagina además el link es poco visible casi nulo.

Figura 8: Mapa del sitio HD

Figura 9: Mapa del sitio2 HD

Índice Global: Posee varios índices a través de la página lo que dificulta diferenciar los temas y la utilización de los mismos.

Figura 10: Índice global HD

Figura 11: Índice global2 HD

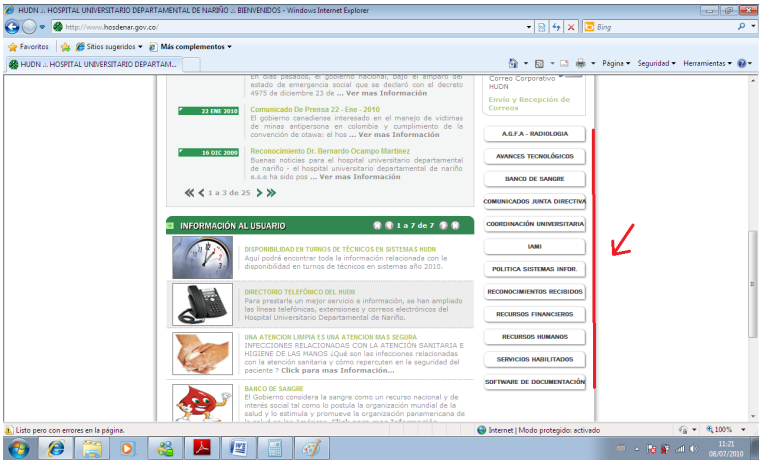


Tabla de Contenidos: La web no contiene tabla de contenido

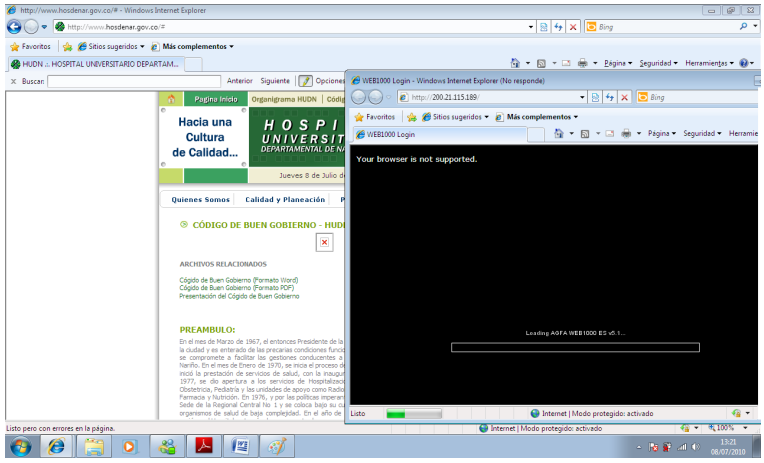
Figura 12: Tabla c HD

Navegabilidad de la página principal: La navegabilidad en la pagina principal se ve afectada por la excesiva cantidad de iconos y de información que hace muy difícil la tarea de encontrar el enlace que se esta buscando además la pagina esta constantemente cambiando los lugares de sus enlaces lo que dificulta la comprensión global de la pagina

Figura 13: Navegabilidad HD

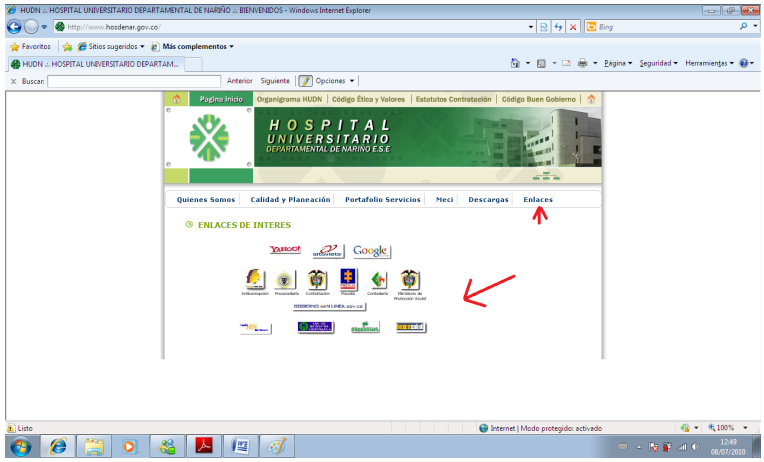
Uniformidad en el Estilo del sitio: El sitio es uniforme en un 90% con algunas excepciones de enlaces a sistemas de información que evitan la plantilla de la web.

Figura 14: Uniformidad HD



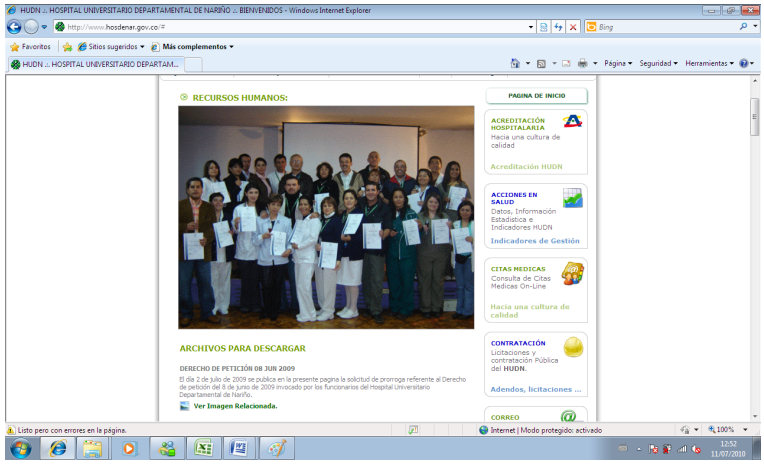
Enlaces a sitios de Interés: El link de enlaces se encuentra activo y actualizado aunque no se discrimina entre sitios de interese general y asociaciones de interés con respecto de la pagina hospitalaria.

Figura 15: Enlaces interés HD



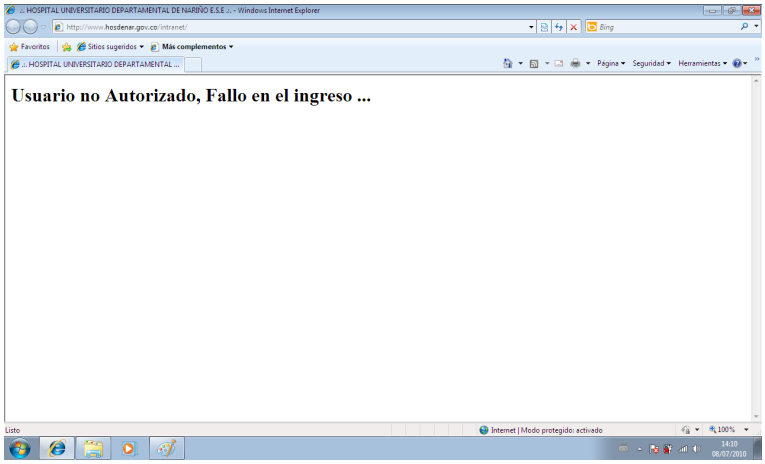
Información sobre los Profesionales: Los profesionales están descritos en la web pero muy superficialmente sin información de contacto ni descritos individualmente

Figura 16: Profesionales HD



Enlaces Rotos: Existen gran cantidad de enlaces rotos en la web

Figura 17: Enlaces rotos HD



A raiz de las evaluaciones descritas anteriormente el equipo auditor plasmo una serie de recomendaciones, junto con el soporte legal que fueron entregados a la entidad Contraloria Departamental de Nariño y que se describen a continuacion.

- **Evaluación de la usabilidad y del decreto 1151 de 2008 de Gobierno en Línea.**

  ✓ **Hospital Civil de Ipiales Decreto 1151 de 2008 de Gobierno en Línea.**

Tabla 36: GL - HC

Nombre de la entidad	HOSPITAL CIVIL DE IPIALES "ESE"
Municipio	IPIALES
Nit	800084362-3
Dirección	AV PANAMERICANA NORTE
Teléfono	7733799
Correo Electrónico	hoscipia@hospitalcivil.com

1. La Entidad cuenta con un sitio Web?	
X	SI
	NO
	En desarrollo
2. Si cuenta con un sitio web, o está en desarrollo escriba la dirección.	
	http://www.hospitalcivil.com/
3. La entidad cuenta con un Comité de Gobierno en línea? Si la respuesta es positiva indicar el acto administrativo y fecha de expedición.	
	SI ACTO ADMINISTRATIVO _____
X	NO
4. Si la respuesta fue SI, relacione los cargos de los integrantes del Comité de Gobierno en Línea:	
	_____
	_____
	_____
	_____
	_____
	_____
5. Con que periodicidad se reúne el comité de Gobierno en línea	
	Mensualmente
	Bimensualmente
	Trimestralmente
	Semestralmente
	Otro CUAL?

Tabla 36: GL – HC (Continuación)

6. El comité realiza un seguimiento sobre la implementación de Gobierno en línea en la entidad?	
	SI
	NO
7. El comité ha realizado algún informe sobre el avance de la implementación de la estrategia del Gobierno en línea.	
	SI
	NO

Las siguientes preguntas pertenecen a la primera Fase de la estrategia (Información en línea), y deberán responderse teniendo en cuenta la inclusión o existencia de la respectiva información, en el sitio Web de la Entidad.

Marcar **SI** cuando el sitio Web contenga la información indicada.
Marcar **NO** cuando el sitio Web no tenga la información indicada.
Marcar **EN DESARROLLO** cuando el ítem respectivo se encuentre en elaboración.

Tabla 37: GL2 – HC

1. Acerca de la Entidad	SI	NO	EN DESARROLLO
a. Misión y visión		X	
b. Objetivos y funciones	X		
c. Organigrama		X	
d. Localización física (incluyendo todas las sedes o sucursales)	X		
e. Teléfonos y/o líneas gratuitas y fax	X		
f. Correo electrónico de contacto		X	
g. Horarios y días de atención al público		X	
h. Directorio de funcionarios principales		X	
i. Directorio de entidades		X	
j. Directorio de agremiaciones y asociaciones	X		
2. Leyes y normatividad vigentes	**SI**	**NO**	**EN DESARROLLO**
a. Leyes/ Ordenanzas /Acuerdos		X	
b. Decretos		X	
c. Resoluciones y/u otros actos administrativos de carácter general		X	

Tabla 37: GL2 – HC (Continuación)

d. Proyectos de normatividad		X	
3. Presupuesto	**SI**	**NO**	**EN DESARROLLO**
a. Presupuesto aprobado en ejercicio de acuerdo con las normas vigentes		X	
b. Información histórica de presupuestos		X	
4. Políticas, planes, programas y proyectos institucionales	**SI**	**NO**	**EN DESARROLLO**
a. Políticas, planes y/o líneas estratégicas		X	
b. Programas y proyectos en ejecución		X	
c. Contacto con dependencia responsable		X	
5. Contratación	**SI**	**NO**	**EN DESARROLLO**
a. Información sobre Licitaciones, selecciones abreviadas, concurso de mérito y Contratación Directa		X	
b. Información sobre Contratos en Ejecución		X	
6. Control y rendición de cuentas	**SI**	**NO**	**EN DESARROLLO**
a. Entes de control que vigilan a la Entidad			X
b. Informes de gestión	X		
c. Metas, indicadores de gestión y/o desempeño y resultados		X	
d. Plan de mejoramiento	X		
7. Servicios de información	**SI**	**NO**	**EN DESARROLLO**
a. Información para niños		X	
b. Preguntas y respuestas frecuentes		X	
c. Boletines y publicaciones			X
d. Noticias			X
e. Calendario de actividades		X	

Tabla 37: GL2 – HC (Continuación)

f. Glosario		X	
g. Política de privacidad y condiciones de uso		X	
8, Estándares de Presentación	**SI**	**NO**	**EN DESARROLLO**
a. Identidad visual (escudo de la República e identidad visual de la Entidad)		X	
b. Enlace al Portal del Estado Colombiano www.gobiernoenlinea.gov.co		X	
c. Fecha de la última actualización del sitio Web		X	
d. División de los contenidos (divididos en porciones pequeñas)	X		
e. Uso de colores (pocos colores, sin caer en un diseño monótono)	X		
f. Manejo de vínculos (textos que indiquen claramente al usuario el contenido de la página Web)	X		
9. Estándares de Funcionalidad	**SI**	**NO**	**EN DESARROLLO**
a. Mapa del sitio		X	
b. Acceso a la página de inicio	X		
c. Acceso al menú principal	X		
10. Estándares Técnicos	**SI**	**NO**	**EN DESARROLLO**
a. Nombre del dominio con formato www.nombredelaentidad.gov.co, .edu.co ó .mil.com		X	
b. Tiempo de despliegue de una página en el navegador de usuario no mayor a 20 segundos	X		
c. Elementos como gráficos o archivos sonoros marcados y/o etiquetados con una descripción de su contenido		X	
d. Elementos gráficos que se muevan, parpadeen se desplacen o se actualicen automáticamente con la posibilidad de ser detenidos temporal o totalmente.		X	

✓ **Usabilidad**

Tabla 38: Usabilidad – HC

Institución:		***HOSPITAL CIVIL DE IPIALES***		
Url:		http://www.hospitalcivil.com/		
Evaluador:		***Luis Carlos Chaves Yela - Ricardo Cabrera Solarte***		
Fecha:		***10/05/2010***		
Nota:		***3,182702381***		
20%		**1. Usabilidad**	**4,968**	**0,9937**
	40%	**1.1 Comprensibilidad Global del Sitio**	**3,733**	**1,4933**
		1.1.1 Esquema de Organización Global	**3,667**	
		1.1.1.1 Mapa del Sitio	1	
		1.1.1.2 Índice Global (por Temas, etc.)	9	
		1.1.1.3 Tabla de Contenidos	1	
		1.1.2 Calidad en el Sistema de Etiquetado	**5**	
		1.1.2.1 Etiquetado Textual	9	
		1.1.2.2 Etiquetado con Iconos	1	
		1.1.3 Visita Guiada	**1**	
		1.1.3.1 Visita Convencional	1	
		1.1.3.2 Visita Virtual (con Tecnología VR)	1	
		1.1.4 Página Principal	**4**	
		1.1.4.1 Navegabilidad de la página principal	6	
		1.1.4.2 Impacto de la página principal	4	
		1.1.4.2.1 La página principal refleja la idea del sitio	5	
		1.1.4.2.2 La página principal deja claro que puedo hacer en el sitio	4	
		1.1.4.2.3 La página principal se ve bien al deshabilitar las imágenes	1	
		1.1.5 Consistencia de la navegación	**5**	
	10%	**1.2 Mecanismos de Ayuda y Retroalimentación en línea**	**4,0**	**0,4**
		1.2.1 Calidad de la Ayuda	**1**	
		1.2.1.1 Ayuda Explicatoria acerca del sitio	1	
		1.2.1.2 Ayuda de la Búsqueda	1	
		1.2.2 Indicador de Ultima Actualización	**5**	
		1.2.2.1 Global (de todo el sitio Web)	1	
		1.2.2.2 Restringido (subsitio o página)	5	
		1.2.2.3 Por noticias (Solo ultimas noticias)	9	
		1.2.3 Directorio de Enlaces	**7,5**	
		1.2.3.1 Enlaces a sitios de Interés	7	

Tabla 38: Usabilidad – HC (Continuación)

		1.2.3.2 Enlaces a asociaciones de interés	8	
		1.2.4 Facilidad FAQ	**1**	
	10%	**1.3 Aspectos de Interfaces y Estéticos**	**8**	**0,8**
		1.3.1 Cohesividad al Agrupar los Objetos de Control Principales	**8**	
		1.3.2 Permanencia y Estabilidad en la Presentación de los Controles Principales	**8**	
		1.3.2.1 Permanencia de Controles Directos	8	
		1.3.2.2 Permanencia de Controles Indirectos	8	
		1.3.2.3 Estabilidad	8	
		1.3.3 Preferencia Estética	**8**	
		1.3.4 Uniformidad en el Estilo del sitio	**8**	
	10%	**1.4 Misceláneas**	**3**	**0,3**
		1.4.1 Soporte a Lenguaje Extranjero	**1**	
		1.4.2 Descarga de contenidos	**3**	
		1.4.2.1 Descarga de contenidos a multidispositivo	1	
		1.4.2.2 Descarga de contenidos	5	
		1.4.3 Intrusión publicitaria	**5**	
	15%	**1.5 Usabilidad de los Textos**	**5,667**	**0,85**
		1.5.1 Textos adaptados para la Web	**5,667**	
		1.5.1.1 Textos breves	8	
		1.5.1.2 Textos escaneables	5	
		1.5.1.3 Estilo de escritura conciso	4	
	15%	**1.6 Clasificación de la información**	**7,5**	**1,125**
		1.6.1 Categorías	7,5	
		1.6.1.1 Claridad de las categorías	8	
		1.6.1.2 Cohesión de las categorías	7	
10%		**2. Accesibilidad**	**1,338**	**0,1338**
	70%	**2.1 Accesibilidad para usuarios con discapacidades**	**1,625**	**1,1375**
		2.1.1 Discapacidades visuales	**2,25**	
		2.1.1.1 Posibilidad de modificar el tamaño de las fuentes	1	
		2.1.1.2 Combinaciones de color (para usuarios con ceguera al color)	6	
		2.1.1.3 Markup claro para poder ser leído por un lector de pantalla	1	
		2.1.1.4 Etiquetas ALT en todas las imágenes	1	
		2.1.2 Discapacidades auditivas	**1**	
	10%	**2.2 Acceso a navegadores no gráficos**	**1**	**0,1**
	10%	**2.3 Acceso Multidispositivo**	**1**	**0,1**

Tabla 38: Usabilidad – HC (Continuación)

15%		**3. Funcionalidad**	**2,875**	**0,4313**
	50%	**3.1 Aspectos de Búsqueda**	**1**	**0,5**
		3.1.1 Mecanismo de Búsqueda en el Sitio	**1**	
		3.1.1.1 Búsqueda Restringida (por secciones)	1	
		3.1.1.2 Búsqueda Global	1	
		3.1.2 Búsqueda siempre disponible	**1**	
	50%	**3.2 Aspectos de Navegación y Exploración**	**4,75**	**2,375**
		3.2.1 Navegabilidad Local (de subsitio)	**1**	
		3.2.1.1 Nivel de Interconexión	1	
		3.2.1.2 Orientación	1	
		3.2.1.2.1 Indicador del Camino	1	
		3.2.1.2.2 Etiqueta de la Posición Actual	1	
		3.2.2 Navegabilidad Global	**4**	
		3.2.2.1 Acoplamiento entre Subsitios	4	
		3.2.3 Objetos de Control Navegacional	**5,75**	
		3.2.3.1 Permanencia y Estabilidad en la Presentación de los Controles Contextuales	7	
		3.2.3.1.1 Permanencia de los Controles Contextuales	7	
		3.2.3.1.2 Estabilidad	7	
		3.2.3.2 Nivel de Desplazamiento	4,5	
		3.2.3.2.1 Desplazamiento Vertical	6	
		3.2.3.2.2 Desplazamiento Horizontal	3	
		3.2.4 Predicción Navegacional	**8**	
		3.2.4.1 Enlace con Título (enlace con texto explicatorio)	8	
		3.2.4.2 Calidad de la Frase del Enlace	8	
		3.2.5 Funciones Misceláneas y Específicas del Dominio	**5**	
40%		**4 Contenidos**	**2,159**	**0,8636**
	20%	**4.1 Información Hospitalaria**	**3,533**	**0,7067**
		4.1.1 Información sobre Servicios	**5**	
		4.1.2 Servicios	**7**	
		4.1.2.1 Planes de servicios actuales	7	
		4.1.1.2 Planes de servicios futuros	7	
		4.1.3 Información sobre las Dependencias	**1**	
		4.1.3.1 Información sobre los Profesionales	1	
		4.1.3.2 Horarios de los Profesionales	1	
		4.1.4 Valores de la Entidad	**3,667**	
		4.1.4.1 Misión y Visión	9	

Tabla 38: Usabilidad – HC (Continuación)

		4.1.4.2 Reglamentos	1	
		4.1.4.3 Historia	1	
		4.1.5 Información sobre Programas Institucionales	1	
		4.1.5.1 Información de Prevención	1	
		4.1.5.2 Programas de Atención	1	
		4.1.5.3 Programas de Salud General	1	
		4.1.5.3 Programas de Especialidades	1	
	15%	**4.2 Información sobre el equipo medico**	**1**	**0,15**
		4.2.1 Hojas de vida de los profesionales	**1**	
		4.2.1.1 Intereses Académicos	1	
		4.2.1.2 Formación	1	
		4.2.2 Areas de los profesionales	**1**	
		4.2.3 Información de contacto	**1**	
		4.2.3.1 Dirección	1	
		4.2.3.2 Teléfono	1	
		4.2.3.3 Mail	1	
		4.2.4 Buscador de profesionales	**1**	
	15%	**4.3 Información sobre Actividades**	**1,333**	**0,2**
		4.3.1 Actividades pasadas	**1**	
		4.3.2 Agenda de actividades futuras	**1**	
		4.3.3 Descripción del evento	**1**	
		4.3.4 Información del ponente	**1**	
		4.3.5 Memoria de actividades realizadas por la institución	**2,667**	
		4.3.5.1 Descripción del evento	4	
		4.3.5.2 Información del ponente	2	
		4.3.5.3 Material utilizado	2	
	20%	**4.4 Información sobre los Programas**	**1**	**0,2**
		4.4.1 Objetivos	**1**	
		4.4.2 Contenidos	**1**	
		4.4.3 Evaluación	**1**	
		4.4.4 Horarios	**1**	
	10%	**4.6 Información de contacto de la Institución**	**1,5**	**0,15**
		4.6.1 Ubicación	**2**	
		4.6.1.1 Como llegar (transportes, distancias, etc.)	4	
		4.6.1.2 Mapa geográfico	1	
		4.6.1.3 Mapa interno	1	
		4.6.2 Contacto con responsables / asesores	**1**	
		4.6.2.1 Nombre	1	
		4.6.2.2 Correo	1	
		4.6.2.3 Teléfono	1	
		4.6.2.4 Fax	1	

Tabla 38: Usabilidad – HC (Continuación)

	10%	**4.7 Información para trabajadores nuevos**	**3,667**	**0,3667**
		4.7.1 Claridad de Misión y Visión	**9**	
		4.7.2 Historia	**1**	
		4.7.3 Reglamento	**1**	
	10%	**4.8 Información para potenciales usuarios**	**3,857**	**0,3857**
		4.8.1 Por que deben elegir este Hospital	**1**	
		4.8.2 Claridad de Misión y Visión	**9**	
		4.8.3 Información geográfica	**1**	
		4.8.4 Información de contacto para obtener mas información	**9**	
		4.8.5 Historia	**1**	
		4.8.6 Reglamento	**1**	
		4.8.7 Organización	**5**	
7,5%		**5. Confiabilidad**	**5,639**	**0,4229**
	50%	**5.1 Ausencia de Deficiencias y Errores**	**7,778**	**3,8889**
		5.1.1 Errores de Enlaces	**7,333**	
		5.1.1.1 Enlaces Rotos	7	
		5.1.1.2 Enlaces Inválidos	8	
		5.1.1.3 Enlaces no Implementados	7	
		5.1.2 Errores o Deficiencias Varias	**9**	
		5.1.2.1 Deficiencias o cualidades ausentes debido a diferentes navegadores	9	
		5.1.2.2 Nodos Web Muertos (sin enlaces de retorno)	9	
		5.1.2.3 Nodos Destinos (inesperadamente) en Construcción	9	
		5.1.3 Enlaces externos a instituciones prestigiosas	**7**	
	25%	**5.2 Utilización de estándares del W3C**	**5**	**1,25**
		5.2.1 HTML	9	
		5.2.2 CSS	1	
	25%	**5.3 Actualización periódica de la información**	**2**	**0,5**
7,5%		**6. Eficiencia**	**4,5**	**0,3375**
	60%	**6.1 Accesibilidad de Información**	**3,5**	**2,1**
		6.1.1 Soporte a Versión sólo Texto	**1**	
		6.1.2 Legibilidad al desactivar la Propiedad Imagen del Browser	**6**	
		6.1.2.1 Imagen con Título	6	
		6.1.2.2 Legibilidad Global	6	
	20%	**6.2 Rendimiento**	**5**	**1**
	20%	**6.3 Tiempo de descarga**	**7**	**1,4**

La nota del sitio web resulto tan baja por que en los siguientes ítems se noto que no cumplieron a cabalidad con las condiciones necesarias de manejo y usabilidad.

- El sitio web no tiene mapa del sitio.
- No se muestra tabla de contenidos.
- No existen etiquetas con iconos.
- No existe visita guiada en esta web.
- No existe visita guiada virtual
- La página principal es muy simple y no llama la atención
- La página principal es poco navegable.
- El impacto es muy bajo porque la combinación de colores es muy mala y existe muy poca información.
- No se tiene una clara idea del sitio en la página principal.
- No se sabe claramente que servicios ofrece la página.
- No existe ayuda en este sitio web.
- No existe indicador de última actualización global
- No existe soporte a Lenguaje Extranjero.
- No existe descarga de contenidos a multidispositivo.
- No hay la posibilidad de modificar el tamaño de las fuentes.
- No existe Markup claro para poder ser leído por un lector de pantalla.
- Las imágenes no contienen etiquetas ALT.
- No existe un mecanismo de búsqueda en el sitio
- No hay disponible información sobre las dependencias.
- No se observan los reglamentos de la entidad.

- No existe información sobre programas institucionales.
- No existe información sobre el equipo médico.
- No existe hojas de vida de los profesionales
- No existe memoria de actividades realizadas por la institución
- Descripción del evento.
- No existe información para trabajadores nuevos
- No existe historia.
- No existe reglamento.
- No existe información geográfica.
- No existe soporte a versión sólo texto.

Figura 18: HC – Usabilidad

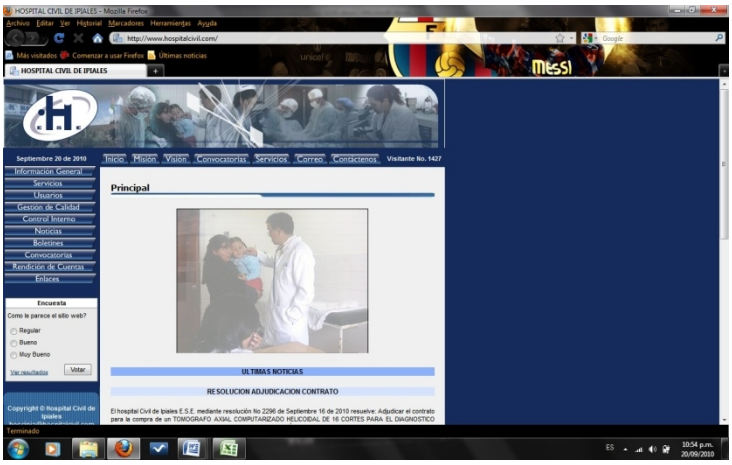


Figura 19: HC – Usabilidad2

Figura 20: HC – Usabilidad3

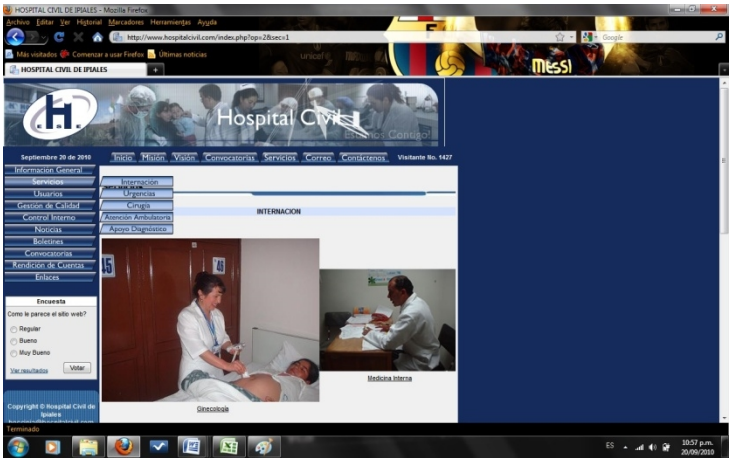


Figura 21: HC – Usabilidad4

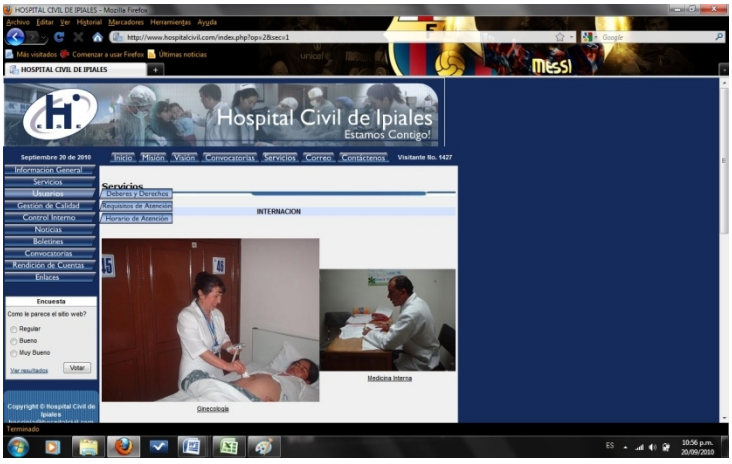
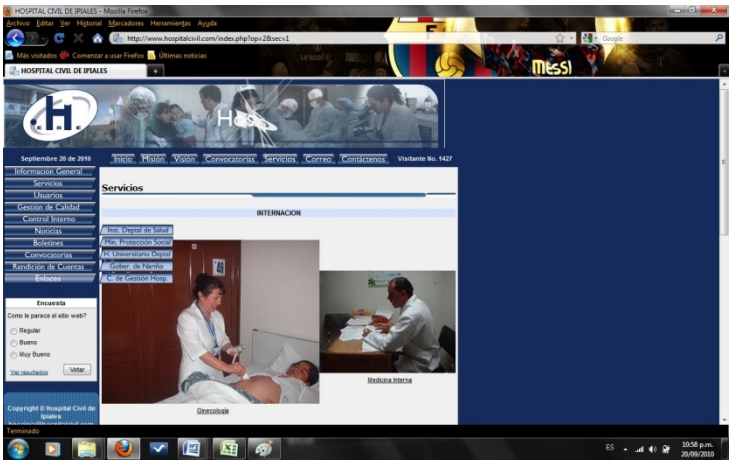


Figura 22: HC – Usabilidad5



4. CONCLUSIONES

- La auditoria de sistemas es la herramienta mas metódica para identificar las vulnerabilidades de una empresa, tanto a nivel físico como a nivel lógico, permite conocer todas las falencias empresariales y propone correcciones para las deficiencias encontradas, muchas veces antes de que esos problemas ocurran, todo esto lo hace con el mayor nivel de responsabilidad, confidencialidad y profesionalismo posible.

- Las herramientas web se han convertido en una de las mayores posibilidades del siglo XXI, ya que pueden llegar a múltiples destinos sin distingo de piel o de raza, es por esto que las entidades del estado deben ser consientes que poseer un portal con los mas altos estándares de calidad es de vital importancia para cumplir con los objetivos de la empresa, por este motivo la Contraloría Departamental de Nariño y el Gobierno Nacional hacen un llamado a las entidades del departamento y del país para cumplir con el decreto 1151 de 2008 de Gobierno en Línea que le permitirá a la sociedad conocer mas a fondo las entidades del estado que les prestan distintos servicios.

- Los funcionarios de las entidades auditadas son consientes de las falencias de su organización y están dispuestos a mejorar los procesos y a aplicar los cambios que la entidad reguladora les pida realizar, por tal motivo todas las recomendaciones son puestas a disposición de la Contraloría Departamental de Nariño para su total manejo y disposición.

- En muchas ocasiones la materia prima de las transacciones y procesos empresariales no es información cien por ciento confiable por lo que es de vital importancia el proceso de auditoria constante con el fin de mejorar todos los procesos que en la entidad se lleven a cabo.

- Las entidades auditadas deben prestar mayor atención al área de sistemas, ya que esta es el soporte y columna de cualquier entidad que preste servicios de información y atención de usuarios, sin esta dependencia muchos de los procesos que ahí se llevan a cabo serian imposibles de sustentar y manejar.

RECOMENDACIONES

- Desarrollar nuevas auditorias a las entidades departamentales que lo requieran, y con la supervisión de entidades como la Contraloría Departamental de Nariño, para su mayor entendimiento y manejo.

- Implementar las metodologías planteadas en este proyecto en las auditorias futuras que se lleven a cabo en la Universidad de Nariño.

- Auditar con mas frecuencia los procesos en entidades gubernamentales ya que estas se encuentran susceptibles a cambios constantes tanto externos como internos.

BIBLIOGRAFIA

CALVO-MANZANO J., CARRILLO J, CUEVAS G, SAN FELIU T, TOVAR E, “Introducción a la Auditoría Informática”, Facultad de Informática de Madrid, 2002.

ECHENIQUE GARCIA José A., Auditoria en informática, 2ª Ed., Mc GRAW-HILL, México D.F., 2005.

Expansión, Control Interno, Auditoría y Seguridad Informática. Tomos II-IV, 1996.

PIATTINI Mario, DEL PESO Emilio, Auditoría en informática: un enfoque práctico, 2ª Ed., Alfaomega/RA-MA, México D.F., 2001.

PINILLA F. José D., Auditoría informática: un enfoque operacional, ECOE, Bogotá, 1995.

L. ZAVARO Y C. MARTÍNEZ, Auditoría informática, las técnicas de auditoría asistidas por computadora (CAAT).

GOVINDAN, MARSHAL, JOHN Y. PICARD, Manifest on Information Systems Control and Management, McGraw-Hill, 1990.

COBOS, Tania Lucía, Universia Colombia y LÓPEZ, Hugo Andrés, Pontificia Universidad Javeriana. Avances en seguridad informática (En línea). En: Universia Colombia. Disponible en la dirección electrónica: http://www.universia.net.co/tesis-de-grado/-matematicas-fisica-y-ciencias-naturales/avances-en-seguridad-informatica.html

ISACA, COBIT 4.1 Castellano (En línea). En: ISACA Colombia (Bogotá). Disponible en la dirección electrónica: http://www.isaca-bogota.net/metodologias/cobit.aspx

WIKIPEDIA. Objetivos de control para la información y tecnologías relacionadas (En línea). En: Wikipedia La enciclopedia Libre. Disponible en la dirección electrónica: http://es.wikipedia.org/wiki/COBIT

WIKIPEDIA. Seguridad Informática (En línea). En: Wikipedia La enciclopedia Libre. Disponible en la dirección electrónica: http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica.

WIKIPEDIA. Organización Internacional para la Estandarización (En línea). En: Wikipedia La enciclopedia Libre. Disponible en la dirección electrónica: http://es.wikipedia.org/wiki/Organizaci%C3%B3n_Internacional_para_la_Estandarizaci%C3%B3n

ANEXOS

Los anexos están dispuestos en un DVD. Estos constan de gran parte de la información obtenida en la investigación, evidencias y el material de base para los hallazgos e informes de este documento.

- **Carpeta Hospital Universitario Departamental de Nariño E.S.E**

Cuadro de Definición de Fuentes:

Archivos CDFHD_01 hasta CDFHD_14

Cuestionarios Cuantitativos

Archivos CCHD_01 hasta CCHD_14

- **Carpeta Hospital Civil de Ipiales E.S.E**

Cuadro de Definición de Fuentes

Archivos CDFHC_01 hasta CDFHC_14

Cuestionarios Cuantitativos

Archivos CCHC_01 hasta CCHC_14

- **Carpeta Imágenes y videos**

Imágenes de las evidencias.

Videos de las evidencias