

**AUDITORÍA INFORMÁTICA A LOS PROCESOS DEL ÁREA DE SISTEMAS  
QUE CONTROLAN LA PARTE ACADÉMICA DEL COLEGIO CHAMPAGNAT  
DE IPIALES – NARIÑO**

**WILLIAM PATIÑO POLANCO  
NELSON ADRIÁN QUIROZ CHAMORRO**

**UNIVERSIDAD DE NARIÑO  
FACULTAD DE INGENIERÍA  
DEPARTAMENTO DE SISTEMAS  
PASTO - NARIÑO  
2016**

**AUDITORÍA INFORMÁTICA A LOS PROCESOS DEL ÁREA DE SISTEMAS  
QUE CONTROLAN LA PARTE ACADÉMICA DEL COLEGIO CHAMPAGNAT  
DE IPIALES – NARIÑO**

**WILLIAM PATIÑO POLANCO  
NELSON ADRIÁN QUIROZ CHAMORRO**

**Trabajo de grado presentado como requisito parcial para optar al título de  
Ingeniero de Sistemas**

**Asesor  
MANUEL ERNESTO BOLAÑOS GONZALEZ  
INGENIERO DE SISTEMAS**

**UNIVERSIDAD DE NARIÑO  
FACULTAD DE INGENIERÍA  
DEPARTAMENTO DE SISTEMAS  
PASTO - NARIÑO  
2016**

## **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 por el Honorable Concejo Directivo de la Universidad de Nariño.

“La Universidad de Nariño no se hace responsable de las opiniones o resultados obtenidos en el presente trabajo y para su publicación priman las normas sobre el derecho de autor”.

Artículo 13, Acuerdo N. 005 de 2010 emanado del Honorable Consejo Académico.

Nota de Aceptación:

---

---

---

---

---

---

---

---

Firma del Presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

San Juan de Pasto, Febrero de 2016.

## **AGRADECIMIENTOS**

Agradezco en primera instancia a Dios, nuestro padre celestial, por hacer posible la realización de este trabajo y darme las capacidades físicas e intelectuales para su correcto desarrollo.

A mis padres Luis Enrique Quiroz Benavides y Ana Ruth del Socorro Chamorro, por ser el apoyo y pilar fundamental para el desarrollo y cumplimiento de todas mis metas, por darme la vida y estar pendientes de ella en todo momento; y por hacer posible la culminación de mis estudios y motivarme a la continuación de ellos.

A mis hermanos Ana Lucia y Luis Carlos, por estar presentes en los momentos alegres y difíciles de mi vida y sentir su apoyo y compañía para mi desarrollo personal y profesional.

A mis hijas Liseth Johana y Angie Lorena, por ser la motivación permanente para salir adelante, por ser el motivo principal de alcanzar mi felicidad y cumplir mi proyecto de vida personal.

A la Universidad de Nariño, por ser parte fundamental de mi formación profesional, por tantos conocimientos y experiencias adquiridas, al rector, administrativos, personal de apoyo y por supuesto, mis queridos docentes, a quienes agradezco todas las enseñanzas recibidas.

A mi Asesor del trabajo de grado, Ingeniero Manuel Bolaños, por su esfuerzo y dedicación, quien con sus conocimientos, su experiencia, su paciencia y su motivación ha logrado en mí que pueda terminar mis estudios con éxito.

A la ingeniera de sistemas María Alicia Pinzón, por su total apoyo en el desarrollo de este proyecto.

Finalmente, mi agradecimiento especial a familiares, amigos y en general a todas aquellas personas que de una u otra forma fueron parte activa para la culminación de mis estudios.

**Nelson Adrián Quiroz Chamorro**

## **AGRADECIMIENTOS**

Agradezco primero que todo a mí Dios, por darme la oportunidad de vivir y existir, su amor y bondad de padre celestial

A mi padre Gilberto Pinchao Patiño, por estar siempre preocupado para que cumpla mis metas y estar pendiente que se una mejor persona cada día.

A mi esposa Deysi Amalfi Posso Guerrero, por estar presente en los momentos alegres y difíciles de mi vida y sentir su amor, apoyo y compañía para mi desarrollo personal y profesional.

A mi hijo Aldhayr Patiño Posso, por ser la motivación permanente para salir adelante, por ser el motor principal de mi felicidad y cumplir mi proyecto de vida personal.

A la Universidad de Nariño, por ser parte fundamental de mi formación profesional, por tantos conocimientos y experiencias adquiridas, al rector, administrativos, personal de apoyo y por supuesto, mis queridos docentes, a quienes agradezco todas las enseñanzas recibidas.

A mi Asesor del trabajo de grado, Ingeniero Manuel Bolaños, por su esfuerzo y dedicación, quien con sus conocimientos, su experiencia, su paciencia y su motivación ha logrado en mí que pueda terminar mis estudios con éxito.

A la ingeniera de sistemas María Alicia Pinzón, por su total apoyo en el desarrollo de este proyecto.

Finalmente, mi agradecimiento especial a familiares, amigos y en general a todas aquellas personas que de una u otra forma fueron parte activa para la culminación de mis estudios.

**William Patiño Polanco**

## **DEDICATORIA**

A Dios,  
por darme la vida, amor, bondad y las capacidades físicas e intelectuales para mi desarrollo personal.

A mis Padres,  
por su apoyo total e incondicional, por sus consejos, sus valores y la motivación constante para formarme como una persona de bien, por la alimentación contante de ese amor fraternal y espíritu de familia.

A mis Hermanos e Hijas,  
por ser parte esencial de mi vida y el apoyo constante para cumplir mis objetivos.

A mis maestros,  
por brindarme tantos conocimientos y experiencias significativas que han hecho crecer personal y profesionalmente.

A mí Asesor,  
Ing. Manuel Bolaños, por su apoyo total para el desarrollo de este proyecto, por su dedicación y el tiempo compartido para nuestra formación profesional.

***Nelson Adrián Quiroz Chamorro***

## **DEDICATORIA**

A Dios,  
por darme todo su amor, bondad y los dones físicos e intelectuales para el desarrollo de mi vida personal.

A mi padre,  
Gilberto Pinchao Patiño, por su total apoyo en todos los proyectos de mi vida.

A mi esposa e Hijo,  
por ser parte esencial de mi vida y el apoyo constante para el cumplimiento de mis objetivos.

A mis maestros,  
por brindarme tantos conocimientos y experiencias significativas que han hecho crecer personal y profesionalmente.

A mí Asesor,  
Ing. Manuel Bolaños, por brindarme todos sus conocimientos, el tiempo necesario y el apoyo total para el desarrollo de este proyecto.

***William Patiño Polanco***

## **RESUMEN**

El desarrollo de este trabajo de grado en modalidad diplomado con presentación de monografía que se llevó a cabo en el Colegio Champagnat de Ipiales-Nariño, consiste en la ejecución de una auditoría a los procesos del área de sistemas que controlan la parte académica de la institución en mención.

Se parte de la necesidad del Colegio para evaluar sus procesos como parte del ciclo PHVA manejado dentro de su sistema de gestión de calidad, la cual la acredita como una institución educativa certificada por ISO 9001.

En cumplimiento de los objetivos de este trabajo de grado se realiza una investigación de las normatividades vigentes en cuanto a procesos del área de sistemas, utilizando como herramienta de auditoría la norma COBIT para lograr generar un informe y brindar una solución integral que ayude a la institución a administrar eficientemente sus procesos, recursos y personal dentro del área de sistemas.

## **ABSTRACT**

The development of this work degree, diploma mode, paper delivered which was performed at Champagnat High School in Ipiales-Nariño, is the execution of an audit processes in the area of systems controlling the academic part of this Institution.

It starts from the need of this Institution to assess their processes as part of PHVA handled within its system of quality management, which accredits it as an educational institution certified by ISO 9001.

To fulfill of the objectives of this paper grade, an investigation of the current regulations about the systems process is made using the COBIT standard as an audit tool to achieve generate a report and provide a comprehensive solution to help the institution to manage efficiently their processes, resources and personnel within the systems area.

## CONTENIDO

	<b>Pág.</b>
INTRODUCCIÓN .....	16
1. PLAN DE AUDITORIA .....	21
1.1 ANTECEDENTES .....	21
1.2 OBJETIVOS .....	21
1.2.1 Objetivo General .....	21
1.2.2 Objetivos Específicos .....	21
1.3 ALCANCES .....	22
1.4 METODOLOGÍA .....	22
1.5 RECURSOS .....	22
1.5.1 Recursos Humanos .....	23
1.5.2 Recursos Físicos .....	23
1.5.3 Recursos Tecnológicos .....	24
1.6 PRESUPUESTO .....	24
1.7 CRONOGRAMA DE ACTIVIDADES .....	25
2. MARCO TEÓRICO .....	26
2.1 MARCO CONCEPTUAL .....	26
2.1.1 Conceptos Generales de la Institución Auditada .....	26
2.1.2 Conceptos Generales de Auditoría Informática .....	28
2.1.3 Herramientas y Técnicas para la Auditoría Informática .....	35
2.1.4 Estándar COBIT: .....	37
2.2 MARCO LEGAL .....	44
3. DESARROLLO DE AUDITORIA .....	48
3.1 ANÁLISIS E INTERPRETACIÓN DE LA INFORMACIÓN .....	48
3.2 MATRIZ DOFA .....	51
3.2.1 Debilidades .....	51

3.2.2	Oportunidades:.....	51
3.2.3	Fortalezas .....	52
3.2.4	Amenazas .....	52
3.3	SELECCIÓN DE DOMINIOS Y PROCESOS.....	52
3.4	ANÁLISIS DE OBJETIVOS DE CONTROL .....	53
3.5	RESUMEN DE NIVEL DE EXPOSICIÓN DE RIESGOS .....	54
3.6	CONTROLES A IMPLEMENTAR PARA PROCESOS EN EL ÁREA.....	55
3.7	PLANES DE ACCION .....	55
3.8	INFORME GENERAL DE LA AUDITORIA.....	56
3.9	INFORME EJECUTIVO DE LA AUDITORÍA.....	59
4.	CONCLUSIONES .....	61
5.	RECOMENDACIONES .....	62
	BIBLIOGRAFIA .....	63
	NETGRAFIA .....	64

## LISTA DE TABLAS

	<b>Pág.</b>
Tabla 1. Presupuesto.....	24
Tabla 2. Cronograma de actividades .....	25
Tabla 3. Dominios y procesos del cobit .....	43
Tabla 4. Resumen de nivel de exposición de riesgos .....	54
Tabla 5. Controles a implementar para procesos en el área .....	55

## LISTA DE ANEXOS

- Anexo No.1: Organigrama institucional
- Anexo No. 2: Horizonte institucional (misión y visión)
- Anexo No. 3: Horizonte institucional (Políticas y objetivos de calidad)
- Anexo No. 4: Factores claves de éxito
- Anexo No. 5: Mapa de procesos
- Anexo No. 6: Perfil y Guía de cargo del asistente de sistemas
- Anexo No. 7: Perfil y Guía de cargo del docente de sistemas y administrador de las aulas de informática
  
- Anexo No. 8: Formatos de encuestas aplicadas a docentes
- Anexo No. 9: Formatos de encuestas aplicadas a estudiantes
- Anexo No. 10: Formatos de encuestas aplicadas a padres de familia
- Anexo No. 11: Formato de entrevista aplicada al administrador de sistemas
- Anexo No. 12: Audio de la entrevista aplicada al administrador de sistemas
- Anexo No. 13: Formato de entrevista aplicada al docente de sistemas y administrador de las aulas de informática
  
- Anexo No. 14: Audio de la entrevista aplicada al docente y administrador de las salas de sistemas
  
- Anexo No. 15: Tabulación de encuestas
- Anexo No. 16: Formatos del desarrollo de la auditoría (Selección de dominios y procesos)
  
- Anexo No. 17: Formatos del desarrollo de la auditoría (Definición de objetivos de control)
  
- Anexo No. 18: Formatos del desarrollo de la auditoría (Planes de acción)
- Anexo No. 19: Informe ejecutivo de la auditoría
- Anexo No. 20: Inventarios y registros fotográficos

## INTRODUCCIÓN

La ingeniería de sistemas comprende diferentes áreas del conocimiento donde se pueden aplicar las distintas técnicas, métodos y recursos propios de ingeniería para la apropiación de nuevas tecnologías.

Es así como la rama de la auditoría de sistemas y la seguridad informática se convierte en un ámbito esencial para administrar la información y los recursos de un sistema informático o un sistema de información.

La evolución de la tecnología condiciona a todo tipo de empresas e instituciones a realizar inversiones económicas para mantener seguridad en su información a través de la buena administración de los procesos que se controlan en el área de sistemas.

A través del desarrollo de este proyecto se auditó los procesos del área de sistemas que controlan la parte académica del Colegio Champagnat de Ipiales – Nariño, realizando un exhaustivo análisis de amenazas, vulnerabilidades y riesgos, utilizando como herramienta de trabajo la norma COBIT, con la cual se confirmó hallazgos para generar un completo informe de auditoría que brinde estrategias y soluciones encaminadas a optimizar cada uno de los procesos del área de sistemas.

A continuación, se describe brevemente el contenido de este documento y se destacan las siguientes partes:

En primer lugar, se citan los aspectos generales, como son modalidad, descripción del problema, formulación del problema, alcance y delimitación, objetivos y justificación para lo cual se fija un cronograma de actividades y se establece un presupuesto.

En segundo lugar, se presenta el marco teórico (marco conceptual y marco legal) del trabajo.

En tercer lugar, se describe la metodología de las actividades desarrolladas en el trabajo de monografía.

En cuarto lugar, se presenta la aplicación de la norma COBIT a los procesos del área de sistemas con el fin de determinar las amenazas, vulnerabilidades y riesgos.

Posteriormente, se presenta el informe final de la auditoría, las conclusiones y se dan a conocer las recomendaciones teniendo en cuenta los hallazgos encontrados brindando las mejores estrategias de solución para la justificación final de este trabajo.

Finalmente, se incluyen los anexos y resultados de las actividades realizadas.

## **MARCO GENERAL DEL PROYECTO**

### **TITULO DEL PROYECTO**

Auditoría informática a los procesos del área de sistemas que controlan la parte académica del Colegio Champagnat de Ipiales – Nariño

### **TEMA**

Auditoria aplicada al área de T.I, en los procesos del sistema informático y de información que controlan la parte académica del Colegio Champagnat de Ipiales-Nariño.

### **MODALIDAD**

Este trabajo de grado, corresponde a la modalidad de TRABAJO DE APLICACION, el cual se realizó en el Colegio Champagnat de Ipiales-Nariño. Trabajo que permitirá acrecentar conocimiento, experiencias y generar diferentes alternativas de desarrollo institucional, por medio de la aplicación de estándares, métodos organizacionales, de funcionamiento, aplicación y cumplimiento de políticas, leyes y normas, necesarias para el buen funcionamiento de una institución y la implementación de buenas prácticas.

### **LINEA DE INVESTIGACION**

Según las líneas de investigación aprobadas y definidas en el Programa de Ingeniería de Sistemas de la Universidad de Nariño, como acuerdo de facultad 045 de octubre 10 de 2002 dado por el consejo de facultad, el proyecto corresponde a la línea de investigación de Sistemas Computacionales, ya que esta línea tiene como objetivo planificar, diseñar, implantar, administrar y evaluar sistemas computacionales y servicios basados en estos sistemas complejos de información, la cual soporta la temática de Auditoria de Sistemas.

### **PLANTEAMIENTO Y DESCRIPCIÓN DEL PROBLEMA**

El Colegio Champagnat de Ipiales es una institución de propiedad de los hermanos maristas cuya misión es prestar el servicio educativo a niños y jóvenes de la ciudad de Ipiales y partes vecinas con una excelente calidad académica y en

procura de formar buenos cristianos y buenos ciudadanos. El Colegio cuenta actualmente con certificación en manejo de procesos ISO 9001 y en procura de lograr la excelencia académica de sus estudiantes desea estar al margen de la tecnología actual, por lo cual cuenta con 2 salas de informática integradas mediante red y con servicios de internet disponibles para un número aproximado de 500 estudiantes y 50 docentes. Además cuenta con un sistema de registro académico de notas (SAPRED) controlado por los docentes y al cual pueden acceder todos los miembros de la comunidad educativa.

La problemática radica en que los procesos que administran la infraestructura tecnológica y el área de sistemas no cuentan con una estructura bien definida. Existen fallas constantes en procesos básicos como mantenimiento de hardware y software, instalación y mantenimiento de la red, copias de seguridad, instalación de software, mantenimiento de usuarios y cuentas, contratación de servicios para el establecimiento. Todo esto conlleva a que no se cumplan las expectativas deseadas para una estructura bien definida dentro del área de sistemas.

Por otra parte, el sistema informático posee debilidades, ya que no existe el personal suficiente para el control de los mismos.

En el mantenimiento de hardware y software cabe mencionar que no existe la documentación pertinente para el debido control de estos procesos. El inventario de equipos no está bien definido, los equipos no cuentan con sus respectivas hojas de vida y no existe la documentación que verifique el soporte y mantenimiento de hardware y software.

En cuanto al proceso de instalación y mantenimiento de la red se observan dificultades en varias terminales de la sala de informática No. 1 y No. 2, los cuales no se encuentran debidamente instaladas, además se observa que existen cables descubiertos y el mantenimiento físico hecho en la sala ha perjudicado las cajillas y terminales RJ45, los cuales se encuentran afectados por la pintura entre otros daños adicionales.

Las backup o copias de seguridad del sistema de información SAPRED, en el cual se registra el rendimiento académico de los estudiantes, no cuenta con las debidas copias de seguridad, las cuales son de responsabilidad del proveedor del servicio; pero de las cuales se debería establecer planes de contingencia por parte del administrador del área de sistemas.

En cuanto a instalación de software se evidencian falencias ya que los sistemas operativos instalados en las máquinas poseen exagerada lentitud en su inicio, a pesar de contar con procesadores CORE I5 y capacidad de memoria RAM de 4 GB. Por otra parte hace falta la instalación de aplicaciones didácticas necesarias y de las cuales la comunidad marista posee las respectivas licencias, así como también existe software que no posee las licencias respectivas.

En el proceso de administración y mantenimiento de cuentas de usuario también se observa múltiples dificultades evidenciadas en que los usuarios no cambian de forma periódica sus claves, algunos, a pesar de llevar tiempo en la Institución, aún no poseen cuentas de acceso para correo electrónico, sistema en línea y sistema de registro a académico SAPRED.

En cuanto a la contratación de servicios se evidencia que el proveedor del sistema SAPRED hace constantes cambios en la plataforma, causando traumatismo en los docentes que son los usuarios directos del sistema, los cambios y el sistema no está debidamente validado y las capacitaciones son cortas y dejan muchas dudas en su manejo. Por la parte de la conectividad existen constantes caídas en el servicio de Internet, el ancho de banda se baja constantemente ya que el contrato es con reuso y no permite el normal desarrollo de las actividades académicas.

Los problemas mencionados anteriormente conllevan a que el control ejercido por el área de sistemas al desarrollo de actividades académicas no se esté llevando de la forma apropiada para prestar el mejor servicio de la Institución y no se cumpla con los estándares de calidad establecidos en el tratamiento de la información.

## **ALCANCE Y DELIMITACIÓN**

Mediante la aplicación de la norma COBIT, la cual permite realizar un análisis exhaustivo de las amenazas, vulnerabilidades y riesgos presentados en cualquier empresa o institución, se desea confirmar los hallazgos dentro de los procesos del área de sistemas que controlan única y exclusivamente la parte académica del Colegio Champagnat de Ipiales-Nariño

## **OBJETIVOS**

### **OBJETIVO GENERAL**

Realizar una auditoría informática para evaluar los procesos del área de sistemas, así como también al personal y documentación que administran la parte académica del Colegio Champagnat de Ipiales –Nariño.

### **OBJETIVOS ESPECIFICOS**

- Realizar un diagnóstico de la forma como se administran los procesos y la documentación del área de sistemas.
- Planear y diseñar instrumentos y pruebas que permitan determinar las causas de los problemas más frecuentes del área de sistemas.

- Ejecutar las pruebas y aplicar los instrumentos diseñados.
- Presentar un informe final de los hallazgos de la auditoría y las respectivas recomendaciones y posibles soluciones a la problemática encontrada.

## **JUSTIFICACIÓN**

La cultura de un país, su progreso y desarrollo siempre estarán relacionados con la planeación de sus procesos educativos, este aspecto se encuentra inmerso en la misión y visión del Colegio Champagnat de Ipiales-Nariño, así como también dentro de su PEI. El colegio siempre desea brindar el mejor desarrollo personal y profesional de sus estudiantes con el objetivo fundamental de formar buenos ciudadanos y buenos cristianos.

Para una buena planeación siempre se hará necesario contar con los diferentes recursos de infraestructura física, tecnológica y humana que permitan desarrollar los procesos de una forma eficaz y eficiente.

El colegio Champagnat de Ipiales – Nariño es una institución educativa certificada por ICONTEC bajo la norma ISO 9001, lo que garantiza la calidad de su servicio.

Académicamente se cuenta con el dato de que en la última década el colegio Champagnat de Ipiales-Nariño se cataloga como el mejor colegio de la ciudad según los resultados de las pruebas ICFES y uno de los 3 mejores colegios a nivel departamental.

El PEI y los procesos académicos del colegio se encuentran debidamente organizados bajo la norma ISO 9001, para lo cual se manejan documentos en línea que sirven como soporte a su buena organización.

Tecnológicamente cuenta con diferentes herramientas que administran su parte financiera y académica.

Todo lo expresado anteriormente y teniendo en cuenta que la parte tecnológica juega un papel fundamental en toda institución, se hizo necesario y justificable la implementación de una auditoría informática a los procesos que controlan la parte académica del colegio Champagnat de Ipiales-Nariño, con el objetivo de establecer planes de mejoramiento enfocados a garantizar la calidad y el ejercicio de las buenas prácticas.

Todo lo anterior con el objetivo fundamental de beneficiar a toda la comunidad educativa (directivos, administrativos, personal de apoyo, docentes, padres de familia y estudiantes) y de esta forma aportar un granito de arena para adquirir la mejor educación de nuestro país.

## 1. PLAN DE AUDITORIA

### 1.1 ANTECEDENTES

Realizando la investigación de los antecedentes de auditorías informáticas llevadas a cabo dentro del Colegio Champagnat de Ipiales, se concluyó que nunca se han ejecutado este tipo de auditorías y sólo se cuentan con registros de auditorías realizadas únicamente a procesos educativos definidos por la norma ISO 9001, quien certificó a la institución desde el año 2013.

Desde el momento de certificación de calidad recibida por el Colegio se vienen desarrollando periódicamente auditorías internas realizadas por la misma institución como precedente para las auditorías realizadas de forma posterior por ICONTEC.

Que esta sea la oportunidad para generar un antecedente como la primera auditoría informática aplicada dentro del Colegio Champagnat de Ipiales – Nariño y se convierta en la base para posteriores auditorías, teniendo en cuenta que dentro de este proyecto se vinculó única y exclusivamente la parte académica, pero destacando que dentro del colegio existen otras áreas que también pueden requerir de un proceso de auditoría.

### 1.2 OBJETIVOS

**1.2.1 Objetivo General.** Evaluar los procesos, el personal y la documentación del área de sistemas que involucran las actividades de registro y control académico del Colegio Champagnat de Ipiales-Nariño.

#### 1.2.2 Objetivos Específicos

- Conocer el área, la infraestructura, los procesos, el personal y la documentación que involucra el área de sistemas del colegio Champagnat de Ipiales-Nariño dentro de los procesos de registro y control académico por parte de los docentes.
- Elaborar un plan de auditoría y diseñar los instrumentos y estrategias para recolectar información y pruebas.
- Aplicar los instrumentos y estrategias diseñadas, realizar las pruebas y

ejecutar el proceso de análisis y evaluación de riesgos para su respectiva valoración.

- Elaborar y entregar el informe final con la lista de riesgos confirmados y controles propuestos como estrategias de solución.

### **1.3 ALCANCES**

#### **De los procesos de área de sistemas se evaluó**

- Existencia de políticas organizacionales, así como también de los procesos básicos de administración del área de sistemas
- Existencia de los procesos de diligenciamiento de actividades de registro y control académico
- Documentación utilizada para cada uno de los procesos
- Instalación y mantenimiento de la infraestructura tecnológica (hardware, software y red)
- Copias de seguridad
- Mantenimiento de usuarios y cuentas
- Capacitación a usuarios finales
- Contratación de servicios para el establecimiento

#### **De la infraestructura tecnológica se evaluó**

- Condiciones físicas y lógicas de los equipos
- Condiciones físicas y lógicas de la red
- Calidad y configuración del equipo servidor
- Calidad de prestadores de infraestructura tecnológica
- Personal responsable de la administración y el mantenimiento de la infraestructura tecnológica

### **1.4 METODOLOGÍA**

A través de una visita programada se conoció mediante observación directa la infraestructura tecnológica del área de sistemas y los procesos que permiten el registro y control académico por parte de los docentes en el sistema informático SAPRED.

Mediante una entrevista programada con el administrador del área de sistemas se indagó sobre la existencia de procesos, documentación y aplicación de los mismos (*ver formato y audio de entrevista en los ANEXOS No. 11 y 12*).

Mediante una entrevista programada con el administrador del aula de informática principal del colegio Champagnat de Ipiales-Nariño, se conoció la situación actual de la infraestructura tecnológica de los equipos, su parte física, su parte lógica, su configuración, las licencias de software, la infraestructura de la red y los problemas más frecuentes relacionados, que impidan el normal desarrollo de las actividades ejecutadas en el aula. Así mismo se tomaron las respectivas pruebas mediante registros fotográficos y de video que permitan observar el estado actual de la estructura física y lógica del aula, los equipos y la red (*ver formato y audio de entrevista en los ANEXOS No. 14 y 15*).

Mediante encuestas aplicadas a los usuarios finales de los procesos de registro y control académico de la comunidad educativa del colegio Champagnat de Ipiales-Nariño (directivos, docentes, padres de familia y estudiantes), se estableció el diagnóstico de los mayores inconvenientes que han evidenciado en la utilización del sistema informático (*ver formatos de encuestas en los ANEXOS No. 8, 9 y 10*)

La auditoría de los procesos estuvo enmarcada bajo el estándar COBIT con lo cual se diseñó un análisis de vulnerabilidades, amenazas y riesgos a través de la descripción de su grado de probabilidad y nivel de impacto.

Teniendo en cuenta los hallazgos encontrados, las pruebas realizadas y los resultados de los instrumentos aplicados se realizó un informe detallado de la situación actual de los procesos del área informática, identificando las causas que originan los mayores riesgos y realizando las sugerencias para su tratamiento y control.

## **1.5 RECURSOS**

**1.5.1 Recursos Humanos.** El equipo auditor estuvo conformado por: William Patiño Polanco y Nelson Adrián Quiroz Chamorro y se apoyó en la ayuda del administrador del aula de informática; Ing. Luis Carlos Quiroz Chamorro y del Asistente de sistemas del Colegio Champagnat Ipiales, Ing. Jaime Alonso Aguirre. De la misma manera se hizo partícipe de la auditoría a los usuarios finales de los procesos de registro y control del sistema académico (directivos, docentes, padres de familia y estudiantes)

### **1.5.2 Recursos Físicos**

- Área principal y equipos donde se llevan a cabo los procesos del área de sistemas
- Área principal y equipos de las salas de informática
- Equipos de la sala de profesores

### 1.5.3 Recursos Tecnológicos

- 1 Equipo servidor de la red
- 40 Estaciones de trabajo distribuidas en 2 salas de informática
- 3Switch distribuidos en la 2 salas de informática
- Red de datos
- 1 Cámara fotográfica
- 1 Video cámara
- 1 Grabadora de audio
- 2 Equipos portátiles
- Sistema operativo del equipo servidor
- Sistema operativo de los equipos usuarios
- Aplicaciones de los usuarios
- Conectividad a internet Banda ancha de 20 MB con reuso

### 1.6 PRESUPUESTO

A continuación, se presenta la tabla de presupuesto estimado para la ejecución de la auditoría informática programada dentro del Colegio Champagnat de Ipiales.

<b>DESCRIPCIÓN</b>	<b>VALOR ESTIMADO</b>
Transporte al sitio de auditoría	\$ 200.000=
Papelería, impresiones y copias	\$ 100.000=
Servicio de internet	\$ 50.000=
Varios e imprevistos	\$ 150.000=
<b>TOTAL</b>	<b>\$500.000=</b>

**Tabla 1. Presupuesto**

## 1.7 CRONOGRAMA DE ACTIVIDADES

ACTIVIDAD	TIEMPO ESTIMADO															
	OCTUBRE			NOVIEMBRE				DICIEMBRE				ENERO				
	S E M 2	S E M 3	S E M 4	S E M 4	S E M 1	S E M 2	S E M 3	S E M 4	S E M 1	S E M 2	S E M 3	S E M 4	S E M 1	S E M 2	S E M 3	S E M 4
Visita programada para conocer la infraestructura tecnológica del área de sistemas y los procesos que permiten el registro y control académico por parte de los docentes en el sistema informático SAPRED.																
Visita programada para entrevista con el administrador del área de sistemas, donde se indagará sobre la existencia de procesos, documentación y aplicación de los mismos.																
Visita programada para entrevista con el administrador de las aulas de informática del colegio Champagnat de Ipiales-Nariño. Recopilación de evidencias fotográficas y de video que permitan observar el estado actual de la estructura física y lógica del aula, los equipos y la red.																
Aplicación de encuestas a los usuarios finales de los procesos de registro y control académico de la comunidad educativa del colegio Champagnat de Ipiales-Nariño (directivos, docentes, padres de familia y estudiantes)																
Aplicación de listas de chequeo que permitan determinar la existencia de los procesos y la documentación apropiada que controla los procesos del área de sistemas.																
Aplicación del estándar COBIT a los procesos identificados (selección de dominios, procesos y objetivos de control)																
Creación del cuadro de análisis de vulnerabilidades, amenazas y riesgos a través de la descripción de su grado de probabilidad y nivel de impacto.																
Diseño de un informe detallado de la situación actual de los procesos del área informática, identificando los hallazgos, las causas que originan los mayores riesgos y realizando las sugerencias para su tratamiento y control.																

**Tabla 2. Cronograma de actividades**

## 2. MARCO TEÓRICO

### 2.1 MARCO CONCEPTUAL

A continuación, se dan a conocer algunos conceptos de términos desconocidos y términos técnicos utilizados dentro de la monografía, con la finalidad de clarificar al lector la terminología utilizada.

#### 2.1.1 Conceptos Generales de la Institución Auditada

**Congregación de los Hermanos Maristas:** La Congregación de los Hermanos Maristas es una congregación religiosa católica que forma parte de la Familia Marista. Fue fundada en La Valla-en-Gier, departamento de Loira (Francia), el 2 de enero de 1817 por san Marcelino Champagnat, un sacerdote de la diócesis de Lyon que fue canonizado el 18 de abril de 1999 por Juan Pablo II.

Los Hermanos Maristas, unos 3800 alrededor del mundo, no son clérigos; de hecho, en la selección de postulantes para el noviciado, nunca se acepta a nadie que tenga aspiraciones de sacerdocio. Ello apunta a asegurar que los internos tengan aptitudes especiales para la misión de educar. Los Hermanos Maristas se dedican a dirigir escuelas primarias y secundarias, universidades, escuelas industriales, orfanatos y casas de acogida en 79 países de los cinco continentes.

El hermano Emili Turú es el actual Superior General de la Congregación, quien reside en Roma<sup>1</sup>.

En Colombia la presencia de los hermanos se dio hace 125 años y poseen diferentes obras en ciudades como Bogotá, Cali, Armenia, Ibagué, Villavicencio, Popayán, Pasto e Ipiales.

---

<sup>1</sup>[https://es.wikipedia.org/wiki/Congregaci%C3%B3n\\_de\\_los\\_Hermanos\\_Maristas](https://es.wikipedia.org/wiki/Congregaci%C3%B3n_de_los_Hermanos_Maristas)

**Sistema de Gestión de Calidad:** Un sistema de gestión de la calidad es una estructura operacional de trabajo, bien documentada e integrada a los procedimientos técnicos y gerenciales, para guiar las acciones de la fuerza de trabajo, la maquinaria o equipos, la información de la organización de manera práctica y coordinada que asegure la satisfacción del cliente y bajos costos para la calidad<sup>2</sup>.

En otras palabras, un sistema de gestión de la calidad es una serie de actividades coordinadas que se llevan a cabo sobre un conjunto de elementos (recursos, procedimientos, documentos, estructura organizacional y estrategias) para lograr la calidad de los productos o servicios que se ofrecen al cliente, es decir, planear, controlar y mejorar aquellos elementos de una organización que influyen en satisfacción del cliente y en el logro de los resultados deseados por la organización.

**Norma ISO 9001:** La ISO 9001:2008 es la base del sistema de gestión de la calidad ya que es una norma internacional y que se centra en todos los elementos de administración de calidad con los que una empresa debe contar para tener un sistema efectivo que le permita administrar y mejorar la calidad de sus productos o servicios<sup>3</sup>.

**Sistema de Información SAPRED:** Sistema Administrador de Procesos Educativos, SAPRED es una herramienta diseñada para funcionar en línea, en donde las instituciones educativas podrán realizar el registro y control académico de sus estudiantes, manteniendo por parte de los docentes un seguimiento continuo de sus avances en las planeaciones institucionales, así como en el registro de las valoraciones; con este sistema también se podrá controlar la asistencia, impuntualidades, aplicar el voto electrónico para la elección del gobierno estudiantil, evaluar la prestación del servicio educativo mediante encuestas en línea<sup>4</sup>.

**Encuestas en Línea:** Una encuesta en línea o encuesta web es una encuesta electrónica realizada en Internet a partir de las respuestas aportadas por los usuarios en un determinado sitio web<sup>5</sup>.

---

<sup>2</sup> [https://es.wikipedia.org/wiki/Sistema\\_de\\_gesti%C3%B3n\\_de\\_la\\_calidad](https://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_calidad)

<sup>3</sup> <http://www.normas9000.com/que-es-iso-9000.html>

<sup>4</sup> <http://www.parquesoftpasto.com/narino-vive-digital-realiza-procesos-de-capacitacion-a-docentes-en-sistema-administrativo-web/>

<sup>5</sup> [https://es.wikipedia.org/wiki/Encuesta\\_web](https://es.wikipedia.org/wiki/Encuesta_web)

**Tic's:** Las Tecnologías de la Información y la Comunicación, también conocidas como TIC, son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Abarcan un abanico de soluciones muy amplio. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes<sup>6</sup>.

### 2.1.2 Conceptos Generales de Auditoría Informática

**Auditoría Informática:** Es la evaluación y verificación de las políticas, controles, procedimientos y la seguridad en general, correspondiente al uso de los recursos de informática por el personal de la empresa (usuarios, informática, alta dirección), a fin de que se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

Según José A. Echenique, la auditoría en informática “es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo o de un sistemas o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles archivos, seguridad y obtención de información. Ello debe incluir los equipos de cómputo como la herramienta que permite obtener la información adecuada y la organización específica que hará posible el uso de los equipos de cómputo”<sup>7</sup>.

**Auditoría de Sistemas:** Desde el punto de vista administrativo, cuando se habla de auditoría sistemas se refiere a los SISTEMAS DE INFORMACIÓN utilizados en las empresas públicas o privadas, mas no al computador como tal, que en sí es una herramienta de los sistemas de información. Se debe tener presente que la administración es un sistema abierto y por tanto cambiante en sus conceptos, técnicas y que está influenciada por lo que acontece en su alrededor.

La auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos

---

<sup>6</sup> <http://www.serviciostic.com/las-tic/definicion-de-tic.html>

<sup>7</sup> <http://auditordesistemas.blogspot.com.co/2011/11/conceptos.html>

los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes; también se puede decir que es el examen y evaluación de los procesos del área de Procesamiento Electrónico de Datos (PED) y de la utilización de los recursos que en ellos intervienen, para llegar a establecer el grado de eficiencia, efectividad y economía de los sistemas computarizados en una empresa y presentar conclusiones y recomendaciones encaminadas a corregir las deficiencias existentes y mejorarlas”<sup>8</sup>.

**Infraestructura Tecnológica:** Conjunto de dispositivos físicos y aplicaciones de software que requiere para operar toda la empresa, así como también los servicios a lo largo y ancho de la empresa, tanto humanas como técnicas.

La Infraestructura tecnológica está compuesta por Hardware, Software, bases de datos, telecomunicaciones, personas y procedimientos todos configurados para recolectar, manipular, almacenar y procesar datos para ser convertidos en información<sup>9</sup>.

**El Hardware:** Corresponde a la estructura física del computador, a sus partes tangibles. Ejemplo de ello es el teclado, pantalla, circuitos, disquetes, etc. Los componentes físicos dependerán de las funciones que se necesiten cumplir, por ejemplo, se requieren mecanismos que permitan:  
Ingresar datos y programas al computador.  
Almacenar datos y programas.  
Procesar la información recibida.  
Entregar datos y programas para ser utilizados por el usuario.

De lo anterior podemos distinguir tres componentes principales del Hardware: Unidad Central de Proceso (CPU), Memoria y Dispositivos de Entrada y Salida<sup>10</sup>.

**Unidad Central de Proceso (CPU) o procesador:** La CPU es la parte 'pensante' o 'inteligente' del computador. Es el encargado de atender las órdenes y datos, realiza las operaciones aritmético-lógicas y controla la operación de los diferentes dispositivos. En la actualidad los mejores procesadores son los de la marca INTEL en sus referencias CORE I5 y CORE I7.

**Memoria:** La Memoria es la encargada de almacenar datos y programas, ya sea por un corto (un rato) o largo (años) período de tiempo. La cantidad de memoria es medida a través de un sistema específico.

La Memoria se divide en dos partes: Memoria Principal y Memoria Secundaria.

---

<sup>8</sup> <http://auditordesistemas.blogspot.com.co/2011/11/conceptos.html>

<sup>9</sup> <http://sistemjarm.blogspot.com.co/2012/05/infraestructura-tecnologica-de-un.html>

<sup>10</sup> <http://www.sccc.co.cl/informatica/conceptos.html>

La Memoria Principal es la unidad de memoria de acceso más rápida de un computador. Para que un computador funcione, todos los datos y programas necesarios deben estar almacenados ('cargados') en la Memoria Principal. Por otro lado, es la memoria de más alto costo, por lo que es limitada en tamaño.

La RAM es la parte de la memoria principal que, a diferencia de la anterior, permite la lectura y escritura de información. Al encender el computador siempre está en blanco (vacía) y es aquí donde se cargan los programas y datos. Además, es una memoria temporal, esto es, si se interrumpe el suministro de energía eléctrica, se pierde el contenido de ésta.

La Memoria Secundaria es una memoria de acceso mucho más lento que la Memoria Principal, es de costo inferior y el almacenamiento de información es permanente e ilimitado. Existe una variedad de dispositivos que cumplen la función de Memoria Secundaria. Los más importantes son: Disquetes y Discos Duros. También existen los discos ópticos y los Compact Disc. En este último tiempo ha aparecido el DVD, de quien se dice vendrá a reemplazar al CD.

El Disco Duro son discos similares a los disquetes, pero más rígidos, de mayor tamaño, mayor capacidad de almacenamiento, mayor velocidad de acceso y de mayor dificultad de ser transportado, debido a que por lo general son instalados en el interior del computador.

**El software:** El software es la parte intangible (físicamente) de un computador. Se utiliza este término para referirse a todo el soporte lógico utilizado por un computador (conjunto de datos y programas).

El software se encuentra dividido en dos grandes grupos: Software de Sistema o Sistema Operativo y Software de Aplicación o Programas Utilitarios.

**Sistema operativo:** Es el conjunto de programas que permiten la interacción (comunicación) entre el usuario y el hardware. Además, hace que el hardware sea utilizable y lo administra de manera de lograr un buen rendimiento<sup>11</sup>.

**Cuentas de Usuario:** En el contexto de la informática, un usuario es una persona que utiliza un sistema informático. Para que los usuarios puedan obtener seguridad, acceso al sistema, administración de recursos, etc. Dichos usuarios deberán identificarse. Para que uno pueda identificarse, el usuario necesita una cuenta (una cuenta de usuario) y un usuario, en la mayoría de los casos asociados a una contraseña. Los usuarios utilizan una interfaz de usuario para acceder a los sistemas, el proceso de identificación es conocido como identificación de usuario o acceso del usuario al sistema (del inglés: "log in")<sup>12</sup>.

---

<sup>11</sup> <http://www.sccc.co.cl/informatica/conceptos.html>

<sup>12</sup> [https://es.wikipedia.org/wiki/Cuenta\\_de\\_usuario](https://es.wikipedia.org/wiki/Cuenta_de_usuario)

**Software de Aplicación:** Corresponde al conjunto de programas que cumple una función específica, con el objeto de solucionar una necesidad particular del usuario, excluyendo las tareas del sistema operativo.

Por ejemplo, si usted quiere escribir textos con una buena presentación, utilizará un Procesador de Texto. Si quiere realizar una gran cantidad de operaciones matemáticas, una Planilla de Cálculo. Si quiere manejar grandes volúmenes de datos, una Base de Datos.

**Base de Datos:** Conjunto organizado de datos e información, la base de datos de una empresa puede contener información de clientes, empleados, inventarios, etc.  
13

**Licencia:** Una licencia de software es un contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciario (usuario consumidor /usuario profesional o empresa) del programa informático, para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas.

Las licencias de software pueden establecer entre otras cosas: la cesión de determinados derechos del propietario al usuario final sobre una o varias copias del programa informático, los límites en la responsabilidad por fallos, el plazo de cesión de los derechos, el ámbito geográfico de validez del contrato e incluso pueden establecer determinados compromisos del usuario final hacia el propietario, tales como la no cesión del programa a terceros o la no reinstalación del programa en equipos distintos al que se instaló originalmente<sup>14</sup>.

**Red de Computadores:** Una red de computadoras, también llamada red de ordenadores, red de comunicaciones de datos o red informática, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios<sup>15</sup>.

**Conector Rj45:** El conector RJ45 (RJ significa Registered Jack) es uno de los conectores principales utilizados con tarjetas de red Ethernet, que transmite información a través de cables de par trenzado. Por este motivo, a veces se le denomina puerto Ethernet<sup>16</sup>.

---

13 <http://sistemjarm.blogspot.com.co/2012/05/infraestructura-tecnologica-de-un.html>

14 [https://es.wikipedia.org/wiki/Licencia\\_de\\_software](https://es.wikipedia.org/wiki/Licencia_de_software)

15 [https://es.wikipedia.org/wiki/Red\\_de\\_computadoras](https://es.wikipedia.org/wiki/Red_de_computadoras)

16 <http://es.ccm.net/contents/187-conector-rj45>

**Servidor:** Un servidor es un equipo informático que forma parte de una red y provee servicios a otros equipos cliente.

Se denomina servidor dedicado, aquel que dedica todos sus recursos a atender solicitudes de los equipos cliente.

Sin embargo un servidor compartido es aquel que no dedica todos sus recursos a servir las peticiones de los clientes, sino que también es utilizado por un usuario para trabajar de forma local<sup>17</sup>.

Existen gran cantidad de tipos de servidores o roles que estos pueden desempeñar. En la siguiente relación enumeramos algunos de los más comunes.

- Servidor de archivos: es aquel que almacena y sirve ficheros a equipos de una red.
- Servidor de Directorio Activo/Dominio: es el que mantiene la información sobre los usuarios, equipos y grupos de una red.
- Servidor de Impresión: se encarga de servir impresoras a los equipos cliente y poner en la cola los trabajos de impresión que estos generan.
- Servidor de Correo: se encarga de gestionar el flujo de correo electrónico de los usuarios, envía, recibe y almacena los correos de una organización.
- Servidor de Fax: gestiona el envío, recepción y almacenamiento de los faxes.
- Servidor Proxy: su principal función es guardar en memoria caché las páginas web a las que acceden los usuarios de la red durante un cierto tiempo, de esta forma las siguientes veces que estos acceden al mismo contenido, la respuesta es más rápida.
- Servidor Web: almacena contenido web y lo pone al servicio de aquellos usuarios que lo solicitan.
- Servidor de Base de Datos: es aquel que provee servicios de base de datos a otros programas o equipos cliente.
- Servidor DNS: permite establecer la relación entre los nombres de dominio y las direcciones IP de los equipos de una red.
- Servidor DHCP: este dispone de un rango de direcciones con el cual, asigna automáticamente los parámetros de configuración de red IP a las máquinas cliente cuando estas realizan una solicitud.
- Servidor FTP: su función es permitir el intercambio de ficheros entre equipos, normalmente su aplicación va muy ligada a los servidores Web<sup>18</sup>.

**Internet:** Internet se podría definir como una red global de redes de ordenadores cuya finalidad es permitir el intercambio libre de información entre todos sus usuarios. Pero sería un error considerar Internet únicamente como una red de

---

<sup>17</sup> <http://www.anerdata.com/que-es-un-servidor.html>

<sup>18</sup> <http://www.anerdata.com/que-es-un-servidor.html>

computadoras. Podemos considerar las computadoras simplemente como el medio que transporta la información. En este caso Internet sería una gran fuente de información práctica y divertida. Con Internet podemos enviar mensajes, programas ejecutables, ficheros de texto, consultar catálogos de bibliotecas, pedir libros, hacer compras, etc.<sup>19</sup>

Hay que tener en cuenta que todos los recursos que se pueden encontrar en Internet existen porque alguna persona de forma voluntaria ha dedicado su tiempo en generarlos.

Internet se basa básicamente en cuatro servicios:

el servicio de correo electrónico (e-mail) que transmite y recibe mensajes: nos podemos poner en contacto con cualquier otro usuario mediante el intercambio de mensajes. Utilizando listas de correo una misma información es enviada a varios destinos al mismo tiempo.

servicio de noticias (news): te suscribes a un grupo de noticias y recibirás información sobre ese tema. Las noticias son almacenadas en un servidor de noticias al que acceden los usuarios interesados.

acceso remoto (telnet): potencialmente puedes conectarte como terminal y establecer una sesión de trabajo en cualquier ordenador (ordenador remoto) de la red si dispones de los permisos de acceso necesarios para acceder a él.

transferencia de ficheros (ftp , File Transfer Protocol o Protocolo de Transferencia de Archivos) que permite transferir archivos de una computadora a otra.

Los clientes de la red pueden ser: usuarios y ordenadores. Los usuarios disponen de un identificador de usuario. Cada ordenador puede darle acceso a la red a uno o varios usuarios, por lo que el identificativo completo de un usuario dentro de Internet se compone del identificador de usuario, seguido de y del identificador del ordenador.

Dentro de Internet es muy importante el tema de la seguridad que debe ser controlado por cada uno de los usuarios. Hay que tener en cuenta que un ordenador puede ser utilizado para a través de él introducirse en otros ordenadores. El mantener la seguridad de nuestra máquina disponemos de las claves de acceso. Elige una clave que pueda recordar pero que no sea obvia<sup>20</sup>.

**Ancho de Banda:** En conexiones a Internet el ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bites por

---

<sup>19</sup> <http://www3.uji.es/~pacheco/INTERN-1.html>

<sup>20</sup> <http://www3.uji.es/~pacheco/INTERN-1.html>

segundo (BPS), kilobytes por segundo (Kbps), o megabytes por segundo (mps).

En las redes de ordenadores, el ancho de banda a menudo se utiliza como sinónimo para la tasa de transferencia de datos - la cantidad de datos que se puedan llevar de un punto a otro en un período dado (generalmente un segundo). Esta clase de ancho de banda se expresa generalmente en bits (de datos) por segundo (bps). En ocasiones, se expresa como bytes por segundo (Bps). Un módem que funciona a 57.600 bps tiene dos veces el ancho de banda de un módem que funcione a 28.800 bps.

En general, una conexión con ancho de banda alto es aquella que puede llevar la suficiente información como para sostener la sucesión de imágenes en una presentación de video.

Debe recordarse que una comunicación consiste generalmente en una sucesión de conexiones, cada una con su propio ancho de banda. Si una de estas conexiones es mucho más lenta que el resto actuará como cuello de botella haciendo lenta la comunicación<sup>21</sup>.

**Ancho de Banda con Reuso:** Reuso no es más que compartir nuestro ancho de banda, entre mayor sea el ancho de banda menos reuso se tiene según lo que he podido averiguar en la empresas proveedoras de Internet. El reuso es la utilización de un ancho de banda con más personas, lo que hacen muchas empresas es utilizar un ancho de banda compartido con otros 4 usuarios es decir que tendríamos una relación 1:5 un canal para 5 personas que si en un momento es usado por esas diez sería dividir el ancho de banda contratado en ese número de personas.

**Backup ó Copia De Seguridad:** Una Copia de Seguridad, es un duplicado de nuestra información más importante, que realizamos para salvaguardar los documentos, archivos, fotos, etc., de nuestro ordenador, por si acaso ocurriese algún problema que nos impidiese acceder a los originales que tenemos en él.

Esta Copia de Seguridad también se denomina Copia de Respaldo e incluso, podremos encontrarnos con la denominación Backup en términos ingleses<sup>22</sup>.

**Sistema Informático:** Un sistema informático es un conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso. Sus partes son: hardware, software y las personas que lo usan.

Por ejemplo, una computadora, sus dispositivos periféricos y la persona que la maneja, pueden constituir un sistema informático.

---

<sup>21</sup> <https://www.masadelante.com/faqs/ancho-de-banda>

<sup>22</sup> <https://basicofacil.wordpress.com/2008/11/03/que-es-una-copia-de-seguridad/>

Un sistema informático puede formar parte de un sistema de información; en este último la información, uso y acceso a la misma, no necesariamente está informatizada. Por ejemplo, el sistema de archivo de libros de una biblioteca y su actividad en general es un sistema de información. Si dentro del sistema de información hay computadoras que ayudan en la tarea de organizar la biblioteca, entonces ese es un sistema informático.

**Diferencia entre Sistema Informático y Sistema de Información:** En un sistema informático se utilizan computadoras para almacenar, procesar y/o acceder a información.

En un sistema de información se pueden utilizar computadoras, pero no es necesario. El acceso a la información puede ser físico (por ejemplo, una persona se encarga de buscar en un archivador).

Tanto el sistema informático como el sistema de información, incluyen a las personas que acceden o producen información dentro del sistema. Las personas tienen que capacitarse para entender el funcionamiento y procedimientos que soporta sistema.

Ambos sistemas tienen un propósito. Por ejemplo, gestionar el acceso y distribución de libros una biblioteca, administrar la entrada/salida de mercadería, personal y otros recursos de un comercio, etc.<sup>23</sup>

**Control:** “Es el conjunto de normas, técnicas, acciones y procedimientos que interrelacionados e interactuando entre sí con los sistemas y subsistemas organizacionales y administrativos, permite evaluar, comparar y corregir aquellas actividades que se desarrollan en las organizaciones, garantizando la ejecución de los objetivos y el logro de las metas institucionales”<sup>24</sup>.

**Matriz DOFA:** Este es un método de análisis y diagnóstico usado para la evaluación de un centro de cómputo, que permite la evaluación del desempeño de los sistemas software, aquí se evalúan los factores internos y externos, para que el auditor puede evaluar el cumplimiento de la misión y objetivo general del área de informática de la organización.<sup>25</sup>

### 2.1.3 Herramientas y Técnicas para la Auditoría Informática

**Observación:** Es una de las técnicas más utilizadas para examinar los diferentes aspectos que intervienen en el funcionamiento del área informática y los sistemas

---

<sup>23</sup> <http://www.alegsa.com.ar/Dic/sistema%20informatico.php>

<sup>24</sup> <http://auditordesistemas.blogspot.com.co/2011/11/conceptos-aplicables-la-auditoria.html>

<sup>25</sup> <http://auditordesistemas.blogspot.com.co/2011/11/tecnicas-e-instrumentos-para-realizar.html>

software, permite recolectar la información directamente sobre el comportamiento de los sistemas, del área de informática, de las funciones y actividades, los procedimientos y operación de los sistemas, y de cualquier hecho que ocurra en el área. En el caso específico de la auditoria se aplica para observar todo lo relacionado con el área informática y los sistemas de una organización con el propósito de percibir, examinar, o analizar los eventos que se presentan en el desarrollo de las actividades del área o de un sistema que permita evaluar el cumplimiento de las funciones, operaciones y procedimientos.

**Entrevistas:** Esta técnica es la más utilizada por los auditores ya que a través de esta se obtiene información sobre lo que está auditando, además de tips que permitirán conocer más sobre los puntos a evaluar o analizar. La entrevista en general es un medio directo para la recolección de información para la captura de los datos informados por medio de grabadoras digitales o cualquier otro medio. En la entrevista, el auditor interroga, investiga y conforma directamente sobre los aspectos que se está auditando. En su aplicación se utiliza una guía general de la entrevista, que contiene una serie de preguntas sobre los temas que se quiere tocar, y que a medida que avanza pueden irse adaptando para profundizar y preguntar sobre el tema.

**Encuestas:** Las encuestas son utilizadas frecuentemente para recolectar información sobre aspectos como el servicio, el comportamiento y utilidad del equipo, la actuación del personal y los usuarios, entre otros juicios de la función informática. No existen reglas para el uso de las encuestas, solo los que regulan los aspectos técnicos y estadísticos tales como la elección del universo y la muestra, que se contemplan dentro de la aplicación de métodos probabilísticas y estadísticos para hacer la mejor elección de las muestras y recolección de opiniones.<sup>26</sup>

**Inventarios:** Consiste en hacer el recuento físico de lo que se está auditando, con el fin de compararla con la que existe en los documentos en la misma fecha. Consiste en comparar las cantidades reales existentes con las que debería haber para comprobar que sean iguales, de lo contrario iniciar la investigación de la diferencia para establecer las causas. Con la aplicación de esta herramienta de la auditoria tradicional, el auditor de sistemas también puede examinar las existencias de los elementos disponibles para el funcionamiento del área informática o del sistema, contabilizando los equipos de cómputo, la información y los datos de la empresa, los programas, periféricos, consumibles, documentos, recursos informáticos, y demás aspectos que se desee conocer, con el fin de comparar la cantidad real con las existencias que se registra en los documentos<sup>27</sup>.

---

<sup>26</sup> <http://auditordesistemas.blogspot.com.co/2011/11/recoleccion-de-informacion-para.html>

<sup>27</sup> <http://auditordesistemas.blogspot.com.co/2011/11/recoleccion-de-informacion-para.html>

#### 2.1.4 Estándar COBIT:

**COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas):** Las mejores prácticas en auditoría recomiendan COBIT como la herramienta estándar para tecnologías de información más utilizada en la ejecución de auditorías; a continuación se explica detalladamente algunos conceptos manejados por ésta y los dominios, procesos y actividades que lo conforman.<sup>28</sup>

**Efectividad:** Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.

**Eficiencia:** Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.

**Confidencialidad:** Se refiere a la protección de información sensible contra divulgación no autorizada.

**Integridad:** Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

**Disponibilidad:** Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

**Cumplimiento:** Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.

**Confiabilidad de la información:** Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

**Datos:** Los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.

**Aplicaciones:** Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.

**Tecnología:** La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.

**Instalaciones:** Recursos para alojar y dar soporte a los sistemas de información.

---

<sup>28</sup> <http://auditordesistemas.blogspot.com.co/2011/11/cobit-objetivos-de-control-para-la.html>

**Personal:** Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

**Niveles de COBIT:** La estructura del estándar COBIT se divide en dominios que son agrupaciones de procesos que corresponden a una responsabilidad personal, procesos que son una serie de actividades unidas con delimitación o cortes de control y objetivos de control o actividades requeridas para lograr un resultado medible<sup>29</sup>.

---

<sup>29</sup> <http://auditordesistemas.blogspot.com.co/2011/11/cobit-objetivos-de-control-para-la.html>

**Distribución de los Dominios y Procesos de COBIT:** La estructura del estándar COBIT se divide en dominios que son agrupaciones de procesos que corresponden a una responsabilidad personal, procesos que son una serie de actividades unidas con delimitación o cortes de control y objetivos de control o actividades requeridas para lograr un resultado medible.

Se definen 34 objetivos de control generales, uno para cada uno de los procesos de las TI. Estos procesos están agrupados en cuatro grandes dominios que se describen a continuación junto con sus procesos y una descripción general de las actividades de cada uno<sup>30</sup>.

DOMINIOS	PROCESOS
<p><b>PLANEACIÓN Y ORGANIZACIÓN (PO):</b>            Cubre la estrategia y las tácticas, se refiere a la identificación de la forma en que la tecnología de la información puede contribuir de la mejor manera al logro de los objetivos de la organización. La consecución de la visión estratégica debe ser planeada, comunicada y administrada desde diferentes perspectivas y debe establecerse una organización y una infraestructura tecnológicas apropiadas.</p>	<p><b>PO1</b> Definir un plan estratégico de TI: El objetivo es lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, para asegurar sus logros futuros.</p> <p><b>PO2</b> Definir la arquitectura de la información: El objetivo es satisfacer los requerimientos de la organización, en cuanto al manejo y gestión de los sistemas de información, a través de la creación y mantenimiento de un modelo de información de la organización.</p> <p><b>PO3</b> Determinar la dirección tecnológica: El objetivo es aprovechar al máximo la tecnología disponible o tecnología emergente, satisfaciendo los requerimientos de la organización, a través de la creación y mantenimiento de un plan de infraestructura tecnológica.</p> <p><b>PO4</b> Definir la organización y relaciones de TI: El objetivo es la prestación de servicios de TI, por medio de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas.</p> <p><b>PO5</b> Manejar la inversión en TI: El objetivo es la satisfacción de los requerimientos de la organización, asegurando el financiamiento y el control de desembolsos de recursos financieros.</p> <p><b>PO6</b> Comunicar las directrices y aspiraciones gerenciales: El objetivo es asegurar el conocimiento y comprensión de los usuarios sobre las aspiraciones de la gerencia, 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.</p> <p><b>PO7</b> Administrar recursos humanos: El objetivo es maximizar las contribuciones del personal a los procesos</p>

<sup>30</sup> <https://sites.google.com/site/auditoriaeninformaticacun/cobit/dominios-y-procesos>

	<p>de TI, satisfaciendo así los requerimientos de negocio, a través de técnicas sólidas para administración de personal.</p> <p><b>PO8</b> Asegurar el cumplir requerimientos externos: El objetivo es 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.</p> <p><b>PO9</b> Evaluar riesgos: El objetivo es asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI, mediante 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.</p> <p><b>PO10</b> Administrar proyectos: El objetivo es 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.</p> <p><b>PO11</b> Administrar calidad: El objetivo es satisfacer los requerimientos del cliente., mediante una planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización.</p>
<p><b>ADQUISICIÓN E IMPLEMENTACIÓN (AI)</b></p> <p>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.</p>	<p><b>AI1</b> Identificar soluciones: El objetivo es asegurar el mejor enfoque para cumplir con los requerimientos del usuario, mediante un análisis claro de las oportunidades alternativas comparadas contra los requerimientos de los usuarios.</p> <p><b>AI2</b> Adquirir y mantener software de aplicación: El objetivo es proporcionar funciones automatizadas que soporten efectivamente la organización mediante declaraciones específicas sobre requerimientos funcionales y operacionales, y una implementación estructurada con entregables claros.</p> <p><b>AI3</b> Adquirir y mantener arquitectura de TI: El objetivo es proporcionar las plataformas apropiadas para soportar aplicaciones de negocios mediante la realización de 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.</p> <p><b>AI4</b> Desarrollar y mantener procedimientos relacionados con TI: El objetivo es asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas</p>

	<p>establecidas, mediante la realización de un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento.</p> <p><b>AI5</b> Instalar y acreditar sistemas: El objetivo es verificar y confirmar que la solución sea adecuada para el propósito deseado mediante la realización de una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas.</p> <p><b>AI6</b> Administrar cambios: El objetivo es minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores, mediante 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.</p>
<p><b>SERVICIOS Y SOPORTE (DS)</b></p> <p>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.</p>	<p><b>DS1</b> Definir niveles de servicio: El objetivo es establecer una comprensión común del nivel de servicio requerido, mediante el establecimiento de convenios de niveles de servicio que formalicen los criterios de desempeño contra los cuales se medirá la cantidad y la calidad del servicio.</p> <p><b>DS2</b> Administrar servicios de terceros: El objetivo es asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos, mediante el establecimiento de 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.</p> <p><b>DS3</b> Administrar desempeño y calidad: El objetivo es asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado, realizando 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.</p> <p><b>DS4</b> Asegurar servicio continuo: El objetivo es mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones, mediante un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio.</p> <p><b>DS5</b> Garantizar la seguridad de sistemas: El objetivo es salvaguardar la información contra usos no autorizados, divulgación, modificación, daño o pérdida, realizando controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados.</p> <p><b>DS6</b> Identificar y asignar costos: El objetivo es asegurar</p>

	<p>un conocimiento correcto atribuido a los servicios de TI realizando un sistema de contabilidad de costos que asegure que éstos sean registrados, calculados y asignados a los niveles de detalle requeridos.</p> <p><b>DS7</b> Capacitar usuarios: El objetivo es asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados realizando un plan completo de entrenamiento y desarrollo.</p> <p><b>DS8</b> Asistir a los clientes de TI: El objetivo es asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente realizando una mesa de ayuda que proporcione soporte y asesoría de primera línea.</p> <p><b>DS9</b> Administrar la configuración: El objetivo es 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 realizando 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.</p> <p><b>DS10</b> Administrar problemas e incidentes: El objetivo es asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder implementando un sistema de manejo de problemas que registre y haga seguimiento a todos los incidentes.</p> <p><b>DS11</b> Administrar datos: El objetivo es asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento, a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI.</p> <p><b>DS12</b> Administrar instalaciones: El objetivo es proporcionar un ambiente físico conveniente que proteja el 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.</p> <p><b>DS13</b> Administrar operaciones: El objetivo es asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada a través de una calendarización de actividades</p>
--	---

	de soporte que sea registrada y completada en cuanto al logro de todas las actividades.
<p><b>MONITOREO (M)</b></p> <p>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.</p>	<p><b>M1</b> Monitorear los procesos: El objetivo es 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.</p> <p><b>M2</b> Evaluar lo adecuado del control interno.: El objetivo es asegurar el logro de los objetivos de control interno establecidos para los procesos de TI.</p> <p><b>M3</b> Obtener aseguramiento independiente: El objetivo es incrementar los niveles de confianza entre la organización, clientes y proveedores externos. Este proceso se lleva a cabo a intervalos regulares de tiempo.</p> <p><b>M4</b> Proveer auditoría independiente: El objetivo es 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.</p>

**Tabla 3. Dominios y procesos del cobit**

**Modelo de Madurez:** El enfoque de los Modelos de Madurez para el control sobre los procesos de TI consiste en desarrollar un método de asignación de puntos para que una organización pueda calificarse desde Inexistente hasta Optimizada (de 0 a 5).<sup>31</sup>

Este planteamiento se basa en el Modelo de Madurez que el Software Engineering Institute definió para la madurez de la capacidad de desarrollo de software. Cualquiera sea el modelo, las escalas no deben estar demasiado simplificadas, lo que haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable.

### **Modelo Genérico de Madurez**

**0 Inexistente:** Total falta de un proceso reconocible. La organización ni siquiera ha reconocido que hay un problema que resolver.

**1 Inicial:** Hay evidencia de que la organización ha reconocido que los problemas existen y que necesitan ser resueltos. Sin embargo, no hay procesos estandarizados pero en cambio hay métodos ad hoc que tienden a ser aplicados en forma individual o caso por caso. El método general de la administración es

<sup>31</sup> <http://www.network-sec.com/gobierno-TI/auditoria-CMM>

desorganizado.

**2 Repetible:** Los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea. No hay capacitación o comunicación formal de procedimientos estándar y la responsabilidad se deja a la persona. Hay un alto grado de confianza en los conocimientos de las personas y por lo tanto es probable que haya errores.

**3 Definida:** Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.

**4 Administrada:** Es posible monitorear y medir el cumplimiento de los procedimientos y emprender acción donde los procesos parecen no estar funcionando efectivamente. Los procesos están bajo constante mejoramiento y proveen buena práctica. Se usan la automatización y las herramientas en una forma limitada o fragmentada.

**5 Optimizada:** Los procesos han sido refinados hasta un nivel de la mejor práctica, basados en los resultados de mejoramiento continuo y diseño de la madurez con otras organizaciones. TI se usa en una forma integrada para automatizar el flujo de trabajo, suministrando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte con rapidez.

Las escalas del Modelo de Madurez ayudarán a la gerencia de usuarios a explicar a los administradores dónde existen deficiencias en la administración de TI y a fijarse objetivos para donde necesitan estar comparando las prácticas de control de su organización con los ejemplos de la mejor práctica. El nivel correcto de madurez estará influenciado por los objetivos de negocio y el entorno operativo de la empresa. Específicamente, el nivel de madurez de control dependerá de la dependencia de TI que tenga la empresa, de la sofisticación de la tecnología y, lo que es más importante, del valor de su información.

## **2.2 MARCO LEGAL**

Dentro de la auditoría llevada a cabo a los procesos del área de sistemas que controlan la parte académica del Colegio Champagnat de Ipiales – Nariño, se aplicó el estándar COBIT, norma legalmente establecida para auditoría a procesos y control de las Tecnologías de la Información.

**Definición de COBIT:** La evaluación de los requerimientos del negocio, los recursos y procesos IT, son puntos bastante importantes para el buen

funcionamiento de una compañía y para el aseguramiento de su supervivencia en el mercado.

El COBIT es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso.

El COBIT es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT y que abarca controles específicos de IT desde una perspectiva de negocios<sup>32</sup>.

Las siglas COBIT significan Objetivos de Control para Tecnología de Información y Tecnologías relacionadas (Control Objectives for Information Systems and related Technology). El modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (Information Systems Auditand Control Association).

**Historia y Evolución:** El proyecto COBIT se emprendió por primera vez en el año 1995, con el fin de crear un mayor producto global que pudiese tener un impacto duradero sobre el campo de visión de los negocios, así como sobre los controles de los sistemas de información implantados. La primera edición del COBIT, fue publicada en 1996 y fue vendida en 98 países de todo el mundo<sup>33</sup>.

Una temprana adición significativa visualizada para la familia de productos COBIT, es el desarrollo de las Guías de Gerencia que incluyen Factores Críticos de Éxito, Indicadores Clave de Desempeño y Medidas Comparativas. Los Factores Críticos de Éxito, identificarán los aspectos o acciones más importantes para la administración y poder tomar, así, dichas acciones o considerar los aspectos para lograr control sobre sus procesos de TI. Los Indicadores Clave de Desempeño proporcionarán medidas de éxito que permitirán a la gerencia conocer si un proceso de TI está alcanzando los requerimientos de negocio. La Medidas Comparativas definirán niveles de madurez que pueden ser utilizadas por la gerencia para: determinar el nivel actual de madurez de la empresa; determinar el nivel de madurez que se desea lograr, como una función de sus riesgos y objetivos; y proporcionar una base de comparación de sus prácticas de control de TI contra empresas similares o normas de la industria. Esta adición, proporcionará herramientas a la gerencia para evaluar el ambiente de TI de su organización con respecto a los 34 Objetivos de Control de alto nivel de COBIT.

---

<sup>32</sup> <http://www.hacienda.go.cr/cifh/sidovih/spaw2/uploads/images/file/COBIT%20audit%20y%20ctrol%20sists%20inf.pdf>

<sup>33</sup> <http://ds5-andre-ortega-5a.host56.com/historia.html>

En definitiva, la organización ISACA (creadora, como ya se ha comentado, de la norma) espera que el COBIT sea adoptado por las comunidades de auditoría y negocio como un estándar generalmente aceptado para el control de las Tecnologías de la Información.

**Legalidad:** ISACA (Information Systems Auditand Control Association) es la entidad internacional legalmente establecida encargada de crear y ejercer control sobre el estándar COBIT.

ISACA promueve activamente la investigación que se traduce en el desarrollo de productos relevantes y útiles para los profesionales de Gobierno de TI, riesgo, control, aseguramiento y seguridad.

ISACA desarrolla y mantiene el internacionalmente reconocido marco de referencia COBIT, ayudar a los profesionales de TI y líderes empresariales a cumplir con sus responsabilidades de gobierno de TI, mientras que la entrega de valor al negocio.

**Estructura:** La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización<sup>34</sup>.

"La adecuada implementación de un modelo COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado.

**Estándares:** El conjunto de lineamientos y estándares internacionales conocidos como COBIT, define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro "dominios" principales, a saber:

**Planificación y organización:** 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 del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse

---

**34** <http://www.monografias.com/trabajos93/cobit-objetivo-contro-tecnologia-informacion-y-relacionadas/cobit-objetivo-contro-tecnologia-informacion-y-relacionadas.shtml>

una organización y una infraestructura tecnológica apropiadas<sup>35</sup>.

**Adquisición e implantación:** 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.

**Soporte y servicios:** 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.

**Monitoreo:** Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda. Estos dominios y objetivos de control facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

---

<sup>35</sup> <http://www.hacienda.go.cr/cifh/sidovih/spaw2/uploads/images/file/COBIT%20audit%20y%20ctrol%20sists%20inf.pdf>

### 3. DESARROLLO DE AUDITORIA

#### 3.1 ANÁLISIS E INTERPRETACIÓN DE LA INFORMACIÓN

Teniendo en cuenta la información recolectada bajo la metodología propuesta en el plan de auditoría se procede a tabular la información para evidenciar los posibles hallazgos como se muestra a continuación: (Ver anexo No. 15)

<b>TABULACIÓN ENCUESTAS DOCENTES</b>							
<b>PREGUNTAS BÁSICAS DE APROPIACIÓN Y USO DE LAS TIC</b>							
No.	PREGUNTA	SI	NO	TOTAL	% SI	% NO	
1	Tiene su propio PC	8	7	15	53,33	46,67	
2	Posee conexión a Internet en su casa	7	8	15	46,67	53,33	
5	Posee correo electrónico	15	0	15	100,00	0,00	
		1	2	3	4	5	TOTAL
3	Desde que sitio accede a Internet	COLEGIO	TRABAJO	VECINO O AMIGO	DIRIGASÉ	OTRO	7
			4		2	1	
4	Tiempo de uso de su computador	NUNCA	MESESUALMENTE	UNA VEZ * SEMANA	2 A 3 VECES * SEMANA	TODOS LOS DÍA	15
		0	2	2	8	3	
6	Hace uso constante de su correo electrónico	NO SABE/NO RESPONDE	NUNCA	RARAS VECES	CASI SIEMPRE	SIEMPRE	15
		0	0	3	8	4	
<b>PREGUNTAS BÁSICAS DE USO Y APROPIACIÓN DE LA HERRAMIENTA SAPRED</b>							
No.	PREGUNTA	SI	NO	TOTAL	% SI	% NO	
7	Conoce de la existencia de sapred	15	0	15	100,00	0,00	
8	Ha recibido capacitación de sapred	15	0	15	100,00	0,00	
		1	2	3	4	5	TOTAL
9	Que valoración le da ud a la capacitación recibida	NO SABE/NO RESPONDE	MALA	REGULAR	BUENO	EXCELENTE	15
		0	0	5	9	1	
10	Que valoración le da ud al programa	NO SABE/NO RESPONDE	MALA	REGULAR	BUENO	EXCELENTE	15
		0	0	0	6	9	
11	Mantiene actualizado el registro académico de los estudiantes en el programa SAPRED	NO SABE/NO RESPONDE	NUNCA	RARAS VECES	CASI SIEMPRE	SIEMPRE	15
		0	0	5	7	3	
12	Sus superiores realizan seguimiento y documentan la actualización del registro en SAPRED	NO SABE/NO RESPONDE	NUNCA	RARAS VECES	CASI SIEMPRE	SIEMPRE	15
		0	0	9	6	0	
13	Encuentra dificultades o errores para el registro académico en SAPRED	NO SABE/NO RESPONDE	NUNCA	RARAS VECES	CASI SIEMPRE	SIEMPRE	15
		0	0	7	8	0	
<b>USO TIC EN LABORES ACADÉMICAS POR PARTE DE DOCENTES Y ESTUDIANTES</b>							
		1	2	3	4	5	TOTAL
		NO SABE/NO RESPONDE	NUNCA	RARAS VECES	CASI SIEMPRE	SIEMPRE	
14	Hace uso de las TIC en el desarrollo de sus clases y actividades académicas	0	0	10	4	1	15
15	Sus estudiantes acogen con gusto la aplicación de las TIC en el desarrollo de sus clases	0	0	8	5	2	15
16	Utiliza las TIC para la preparación de sus clases	0	0	8	3	4	15
17	Con que frecuencia piensa que sus estudiantes copian de Internet información sin citar sus fuente	0	0	3	4	8	15
18	Cree que los padres realizan seguimiento de las actividades que realizan los estudiantes en Internet	0	0	9	6	0	15
<b>PREGUNTAS BÁSICAS DE USO Y APROPIACIÓN DE LA PAGINA WEB DEL COLEGIO</b>							
		1	2	3	4	5	TOTAL
19	Cada cuanto visita la pagina web	NO SABE/NO RESPONDE	NUNCA	RARAS VECES	CASI SIEMPRE	SIEMPRE	15
		0	0	10	4	1	
20	Como evalúa la página web	NO SABE/NO RESPONDE	MALA	REGULAR	BUENO	EXCELENTE	15
		0	0	3	10	2	
<b>PREGUNTAS BÁSICAS DE USO Y APROPIACIÓN DE LOS DOCUMENTOS DE SGC</b>							
		SI	NO	TOTAL	% SI	% NO	
21	Conoce donde se encuentran los documentos del SGC	15	0	15	100,00	0,00	
		1	2	3	4	5	TOTAL
22	Cada cuanto visita o descarga los documentos en línea que se manejan en el SGC	NO SABE/NO RESPONDE	NUNCA	RARAS VECES	CASI SIEMPRE	SIEMPRE	15
		0	0	9	6	0	

CAMBIOS DE CONTRASEÑA							
		1	2	3	4	5	TOTAL
		NO SABE/NO RESPONDE	NUNCA	RARAS VECES	CASI SIEMPRE	SIEMPRE	
23	Cada cuanto cambia la contraseña de su correo institucional	0	10	3	2	0	15
24	Cada cuanto cambia la contraseña de sus cuenta de usuario de SAPRED	0	9	5	1	0	15
25	Cada cuanto cambia su contraseña para acceder a los documentos en línea del SGC	0	13	1	1	0	15

VALORACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA POR PARTE DE LOS PADRES DE FAMILIA							
No.	PREGUNTA	1	2	3	4	5	TOTAL
		NO SABE/NO RESPONDE	MALA	REGULAR	BUENO	EXCELENTE	
26	Cómo evalúa el funcionamiento de los equipos de computo	0	0	7	8	0	15
27	Cómo evalúa el funcionamiento de la red (cableado y wifi)	0	0	6	9	0	15
28	Cómo evalúa el servicio de Internet contratado en el colegio	0	0	5	10	0	15
29	Cómo evalúa el personal que presta apoyo tecnológico dentro del colegio	0	0	1	9	5	15

## TABULACIÓN ENCUESTAS PADRES DE FAMILIA

PREGUNTAS BÁSICAS DE APROPIACIÓN Y USO DE LAS TIC						
No.	PREGUNTA	SI	NO	TOTAL	% SI	% NO
1	Tiene su propio PC	57	9	66	86,36	13,64
2	Posee conexión a Internet en su casa	59	7	66	89,39	10,61
4	Posee correo electrónico	59	7	66	89,39	10,61

		1	2	3	4	5	TOTAL
		COLEGIO	TRABAJO	VECINO O AMIGO	CIFERCAFÉ	OTRO	
3	Desde que sitio accede a Internet		4		2	1	7

PREGUNTAS BÁSICAS DE USO Y APROPIACIÓN DE LA HERRAMIENTA SAPRED						
No.	PREGUNTA	SI	NO	TOTAL	% SI	% NO
5	Conoce de la existencia de sapred	60	6	66	90,91	9,09
6	Ha recibido capacitación de sapred	22	44	66	33,33	66,67
8	Realiza seguimiento a través de sapred	36	30	66	78,26	45,45

		1	2	3	4	5	TOTAL
		NO SABE/NO RESPONDE	MALA	REGULAR	BUENO	EXCELENTE	
7	Que valoración le dá ud al programa	15		9	33	9	66
9	Cada cuanto tiempo realiza seguimiento	1	4	15	14	4	38

PREGUNTAS BÁSICAS DE USO Y APROPIACIÓN DE LA PAGINA WEB DEL COLEGIO						
No.	PREGUNTA	SI	NO	TOTAL	% SI	% NO
10	Conoce la página web del colegio	51	15	66	77,27	22,73

		1	2	3	4	5	TOTAL
		NO SABE/NO RESPONDE	NUNCA	RARAS VECES	CASI SIEMPRE	SIEMPRE	
11	Cada cuanto visita la pagina web	6	13	30	13	4	66
12	Como evalúa la página web	22		2	38	4	66

USO TIC EN LABORES ACADÉMICAS POR PARTE DE DOCENTES Y ESTUDIANTES						
No.	PREGUNTA	SI	NO	TOTAL	% SI	% NO
13	Conoce si los docentes utilizan las TIC en el desarrollo de sus clases	41	25	66	89,13	54,35

		1	2	3	4	5	TOTAL
		NO SABE/NO RESPONDE	NUNCA	RARAS VECES	CASI SIEMPRE	SIEMPRE	
14	Con que frecuencia los docentes hacen uso de las TIC	23	2	8	28	5	43
15	Con que frecuencia observa a su hijo hacer uso de las TIC para el desarrollo de labores académicas	6	9	14	23	14	66
16	Realiza seguimiento a las actividades que su hijo(a) realiza en Internet	3	2	13	32	16	66

VALORACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA POR PARTE DE LOS PADRES DE FAMILIA							
No.	PREGUNTA	1	2	3	4	5	TOTAL
		NO SABE/NO RESPONDE	MALA	REGULAR	BUENO	EXCELENTE	
17	Cómo evalúa el funcionamiento de los equipos de computo	6	3	5	43	9	66
18	Cómo evalúa el funcionamiento de la red (cableado y wifi)	18	2	10	33	3	66
19	Cómo evalúa el servicio de Internet contratado en el colegio	18	3	7	33	5	66
20	Cómo evalúa el personal que presta apoyo tecnológico dentro del colegio	13	1	5	31	16	66

# TABULACIÓN ENCUESTAS ESTUDIANTES

## PREGUNTAS BÁSICAS DE APROPIACIÓN Y USO DE LAS TIC

No.	PREGUNTA	SI	NO	TOTAL	% SI	% NO
1	Tiene su propio PC	36	10	46	78,26	21,74
2	Posee conexión a Internet en su casa	38	8	46	82,61	17,39
5	Posee correo electrónico	43	3	46	93,48	6,52

  

	1	2	3	4	5	TOTAL	
3	Desde que sitio accede a Internet	COLEGIO	CASA FAMILIAR	VECINO O AMIGO	OFERCAFÉ	OTRO	10
	0	4	1	2	3		
4	Tiempo de uso de su computador	NUNCA	MENSUALMENTE	UNA VEZ * SEMANA	2 A 3 VECES * SEMANA	TODOS LOS DÍAS	46
	2	2	6	31	5		
6	Envía correos a sus docentes para aclarar dudas	NO SABE/NO RESPONDE	NUNCA	RARAS VECES	CASI SIEMPRE	SIEMPRE	46
	0	10	26	5	5		

## PREGUNTAS BÁSICAS DE USO Y APROPIACIÓN DE LA HERRAMIENTA SAPRED

No.	PREGUNTA	SI	NO	TOTAL	% SI	% NO
7	Conoce de la existencia de sapred	46	0	46	100,00	0,00
8	Ha recibido capacitación de sapred	23	23	46	50,00	50,00
10	Realiza seguimiento a través de sapred	41	5	46	89,13	10,87

  

	1	2	3	4	5	TOTAL	
9	Que valoración le da ud al programa	NO SABE/NO RESPONDE	MALA	REGULAR	BUENO	EXCELENTE	46
	0	0	7	29	10		
11	Cada cuanto tiempo realiza seguimiento	CASI NUNCA	RARA VEZ	CADA PERIODO	MENSUALMENTE	SEMANALMENTE	46
	4	6	26	5	5		

## PREGUNTAS BÁSICAS DE USO Y APROPIACIÓN DE LA PAGINA WEB DEL COLEGIO

No.	PREGUNTA	SI	NO	TOTAL	% SI	% NO
12	Conoce la página web del colegio	44	2	46	95,65	4,35

  

	1	2	3	4	5	TOTAL	
13	Cada cuanto visita la pagina web	NO SABE/NO RESPONDE	NUNCA	RARAS VECES	CASI SIEMPRE	SIEMPRE	46
	1	11	29	5	1		
14	Como evalúa la página web	NO SABE/NO RESPONDE	MALA	REGULAR	BUENO	EXCELENTE	46
	3	0	9	29	5		

  

No.	PREGUNTA	SI	NO	TOTAL	% SI	% NO
7	Conoce de la existencia de sapred	46	0	46	100,00	0,00
8	Ha recibido capacitación de sapred	23	23	46	50,00	50,00
10	Realiza seguimiento a través de sapred	41	5	46	89,13	10,87

  

	1	2	3	4	5	TOTAL	
9	Que valoración le da ud al programa	NO SABE/NO RESPONDE	MALA	REGULAR	BUENO	EXCELENTE	46
	0	0	7	29	10		
11	Cada cuanto tiempo realiza seguimiento	CASI NUNCA	RARA VEZ	CADA PERIODO	MENSUALMENTE	SEMANALMENTE	46
	4	6	26	5	5		

## PREGUNTAS BÁSICAS DE USO Y APROPIACIÓN DE LA PAGINA WEB DEL COLEGIO

No.	PREGUNTA	SI	NO	TOTAL	% SI	% NO
12	Conoce la página web del colegio	44	2	46	95,65	4,35

  

	1	2	3	4	5	TOTAL	
13	Cada cuanto visita la pagina web	NO SABE/NO RESPONDE	NUNCA	RARAS VECES	CASI SIEMPRE	SIEMPRE	46
	1	11	29	5	1		
14	Como evalúa la página web	NO SABE/NO RESPONDE	MALA	REGULAR	BUENO	EXCELENTE	46
	3	0	9	29	5		

## USO TIC EN LABORES ACADÉMICAS POR PARTE DE DOCENTES Y ESTUDIANTES

No.	PREGUNTA	SI	NO	TOTAL	% SI	% NO
15	Los docentes utilizan las TIC en sus clases	44	2	46	95,65	4,35

  

	1	2	3	4	5	TOTAL	
16	Con que frecuencia los docentes hacen uso de las TIC	NO SABE/NO RESPONDE	NUNCA	RARAS VECES	CASI SIEMPRE	SIEMPRE	46
	2	0	19	24	3		
17	Con que frecuencia tus docentes te solicitan que hagas uso de las TIC	2	3	16	25	0	46
18	Con que frecuencia utiliza usted las TIC para desarrollar labores académicas	1	2	17	25	1	46
19	Has reflexionado sobre la calidad de información que encuentra en Internet	0	3	19	22	2	46
20	Frecuencia para copiar de Internet sin citar la fuente	2	0	3	31	10	46
21	Sus padres realizan seguimiento a las actividades que usted realiza en Internet	1	9	11	13	12	46

## VALORACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA POR PARTE DE LOS ESTUDIANTES

No.	PREGUNTA	1	2	3	4	5	TOTAL
		NO SABE/NO RESPONDE	MALA	REGULAR	BUENO	EXCELENTE	
22	Cómo evalúa el funcionamiento de los equipos de computo	0	1	7	30	8	46
23	Cómo evalúa el funcionamiento de la red (cableado y wifi)	4	5	13	21	3	46
24	Cómo evalúa el servicio de Internet contratado en el colegio	4	2	15	22	3	46
25	Cómo evalúa el personal que presta apoyo tecnológico dentro del colegio	2	0	3	27	14	46

## **3.2 MATRIZ DOFA**

### **3.2.1 Debilidades**

- El Colegio Champagnat de Ipiales no tiene bien definidos los procesos del área de sistemas
- No existe un inventario estructurado de la herramientas tecnológicas con las que se cuenta
- Los procesos no se encuentran debidamente documentados
- No existen mantenimiento preventivo para la infraestructura tecnológica (servidores, usuarios, red de datos), tan solo se acude cuando se presentan fallas
- Los equipos no poseen su respectiva hoja de vida
- El personal con que se cuenta dentro del área de sistemas no es el suficiente
- Existe inseguridad debido a la falta de mantenimiento de cuentas de usuario
- Falta capacitación de usuarios para el manejo del sistema SAPRED, especialmente cuando se realizan modificaciones
- Errores en la administración de roles y permisos para acceso a los documentos en línea del sistema de gestión de calidad
- Desactualización de la página web institucional
- Falta de equipos de cómputo para los usuarios de la institución (docentes y estudiantes)
- Ambigüedad de la red de datos y la red eléctrica
- Problemas de configuración de los equipos de computo
- Instalación de software sin sus respectivas licencias

### **3.2.2 Oportunidades:**

- Definir correctamente los procesos del área de sistemas con el apoyo de una norma que optimice el funcionamiento del área
- Apoyarse en internet para el manejo de documentos en línea de los procesos del área de sistemas
- Contratar el servicio externo de mantenimiento preventivo para toda la infraestructura tecnológica
- Capacitar a los usuarios para control, administración y seguridad de sus cuentas de usuario para accesos a los diferentes sistemas
- Capacitación constante por parte de la empresa diseñadora del sistema de registro y seguimiento académico SAPRED
- Adquisición de nuevos equipos de computo
- Migración de la red de datos a una categoría que ofrezca mayor velocidad
- Verificación de las licencias de software y uso de software libre

### **3.2.3 Fortalezas**

- Institución con trascendencia dentro de la ciudad de Ipiales
- Amplia y buena infraestructura física de la institución
- Manejo de documentación y evidencias de procesos educativos debido a la certificación de calidad ICONTEC ISO 9001
- Tiene bien definidos los perfiles y guías de cargo de cada uno de los colaboradores
- Espacio suficiente para las 2 salas de informática
- Contar con sistemas de información como SAPRED para registro y seguimiento académico
- Tener su respectiva página web institucional dentro de la nube
- Manejar y administrar documentos en línea del sistema de gestión de calidad

### **3.2.4 Amenazas**

- Rotación constante del personal que atiende el área de sistemas
- Bajas de equipos de cómputo por falta de mantenimiento
- Problemas legales por licencias de software
- Falla en la integridad de la información dentro del sistema de registro y control académico SAPRED
- Pérdida de confidencialidad de información por la mala administración de cuentas de usuario
- Violación de la seguridad dentro de las aplicaciones utilizadas dentro de la institución
- Deficiente nivel de eficacia y eficiencia en la conectividad a Internet
- Pérdida de información por falta de creación periódica de copias de seguridad

## **3.3 SELECCIÓN DE DOMINIOS Y PROCESOS**

Con base en el análisis de la información recopilada se realizó el análisis COBIT, seleccionando en primera instancia los dominios y procesos, teniendo en cuenta los alcances de la auditoría citados en la metodología; además se determina su estado de madurez actual y el estado proyectado. Para lo anterior se utilizó el siguiente formato:

<b>MODELO DE MEJORES PRACTICAS – COBIT</b>			
<b>EMPRESA :</b> Colegio Champagnat Ipiales		<b>Fecha de diagnóstico:</b> Dic./ 2015	
<b>Diseño de un Sistema de Gestión de Seguridad</b>			
<b>MODELO DE MADUREZ</b>			
<b>DOMINIO:</b> NOMBRE DEL DOMINIO		<b>Código -</b> Nombre del proceso	
<b>OBJETIVO DE CONTROL</b>			
Descripción del objetivo de control			
Estado Actual :	Calificación	Estado Proyectado:	Calificación
<b>CRITERIOS DE CALIFICACIÓN</b>			
<b>0</b>	<b>Inexistente</b>		
<b>1</b>	<b>Inicial /Ad Hoc</b>		
<b>2</b>	<b>Repetible pero Intuitivo</b>		
<b>3</b>	<b>Proceso Definido</b>		
<b>4</b>	<b>Administrado y Medible</b>		
<b>5</b>	<b>Optimizado</b>		

**VER DESARROLLO EN EL ANEXO No. 16**

### **3.4 ANÁLISIS DE OBJETIVOS DE CONTROL**

Una vez realizado el análisis COBIT para selección de dominios y procesos se realizó el análisis de cada uno de los objetivos de control, su grado de ocurrencia, nivel de impacto y nivel de riesgo para cada uno de los dominios y procesos seleccionados previamente; finalmente, se justifica aquellos objetivos de control que presentan mayor nivel de riesgo, como se muestra en el siguiente formato:

MODELO DE MEJORES PRACTICAS – COBIT					
EMPRESA : Colegio Champagnat Ipiales			Fecha de diagnóstico: Dic./ 2015		
OBJETIVOS DE CONTROL		OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
CODIGO PROCESO	NOMBRE PROCESO	DESCRIPCIÓN OBJETIVO DE CONTROL			

**VER DESARROLLO EN EL ANEXO No. 17**

### 3.5 RESUMEN DE NIVEL DE EXPOSICIÓN DE RIESGOS

A continuación se detalla un resumen del nivel de exposición de los riesgos, teniendo en cuenta el impacto de cada uno de los procesos en el objetivo general de la auditoría.

Procesos	Objetivos de Control	Alto	Medio	Bajo	Alto + Medio
DS4 - Asegurar continuidad del servicio	13	6	4	3	10
DS5 - Garantizar la seguridad de sistemas	21	1	8	12	9
DS11 - Administrar la información	30	0	7	23	7
PO9 - Evaluar Riesgos	8	0	6	2	6
PO11 -Administrar Calidad	19	0	6	13	6
DS12 - Administrar las instalaciones	6	1	3	2	4
AI6 - Administrar cambios	8	0	2	6	2
	105	8	36	61	44
		8%	34%	58%	42%

**Tabla 4. Resumen de nivel de exposición de riesgos**

### 3.6 CONTROLES A IMPLEMENTAR PARA PROCESOS EN EL ÁREA

Los controles a implementar están enfocados a los siguientes procesos de Administración de IT.

DOMINIO		PROCESO	
Planeación y Organización	y	PO9	Evaluar riesgos
		PO11	Administrar Calidad
Adquisición e Instalación	e	AI6	Administrar cambios
Entrega de Servicios	de	DS4	Asegurar continuidad del servicio
		DS5	Garantizar la seguridad de sistemas
		DS11	Administrar la información
		DS12	Administrar las instalaciones

**Tabla 5. Controles a implementar para procesos en el área**

### 3.7 PLANES DE ACCION

En este ítem se definen los planes de acción para mitigar las amenazas, vulnerabilidades y riesgos según la definición de los hallazgos demostrados. Para ello se utilizó el siguiente formato:

MODELO DE MEJORES PRACTICAS – COBIT			
EMPRESA : Colegio Champagnat Ipiales		Fecha de diagnóstico: Dic./2015	
Diseño de un Sistema de Gestión de Seguridad			
PLAN DE ACCIÓN			
DOMINIO :	NOMBRE DEL DOMINIO	PROCESO:	CODIGO – NOMBRE DEL PROCESO
CONTROLES			
Control a Implementar COD PROCESO COD CONTROL	DEFINICIÓN DE UN MARCO REFERENCIAL DE RIESGOS		
	Descripción del plan de acción		
Responsables de implementación	Persona o personas que ejecutarán el plan		

<b>Plazo (tiempo de ejecución)</b>	Tiempo establecido para el plan						
<b>MATRIZ DE RESUMEN</b>							
<b>RIESGOS A MITIGAR</b>							
Objetivos de Control	Riesgo Actual			Riesgo Esperado			OBSERVACIÓN
	O	I	T	O	I	T	

**VER DESARROLLO EN EL ANEXO No. 18**

### **3.8 INFORME GENERAL DE LA AUDITORIA**

#### **Identificación del Informe**

Auditoria de procesos del área de sistemas

#### **Identificación del Cliente**

Área de Sistemas Colegio Champagnat Ipiales - Nariño

#### **Identificación de la Entidad Auditada**

Colegio Champagnat de Ipiales NIT. 860006744-9

#### **Objetivos**

Verificar si existen procesos y políticas administrativas para el área de sistemas del involucran las actividades de registro y control académico del colegio Champagnat de Ipiales-Nariño.

#### **Hallazgos Potenciales**

- Falta de procesos en el área de sistemas para el registro en aplicativo SAPRED
- Falta control sobre software SAPRED
- No existe un calendario de mantenimiento SAPRED
- Falta mecanismos de control y comunicación directa con contratista que

permita la solución de inconvenientes que refieran al sistema SAPRED

- No existen políticas claras sobre el uso de medios tecnológicos
- No existe un calendario programado de manteniendo de infraestructura tecnológica

### **Alcance de la Auditoria**

#### **De los procesos de área de sistemas se evaluó**

- Existencia de políticas organizacionales para cada uno de los procesos
- Existencia de los procesos básicos de administración del área de sistemas
- Existencia de los procesos de diligenciamiento de actividades de registro y control académico
- Documentación utilizada para cada uno de los procesos
- Instalación y mantenimiento de hardware y software
- Instalación y mantenimiento de la red
- Copias de seguridad
- Mantenimiento de usuarios y cuentas
- Capacitación a usuarios finales
- Contratación de servicios para el establecimiento

#### **De la infraestructura tecnológica se evaluó**

- Condiciones físicas y lógicas de los equipos
- Condiciones físicas y lógicas de la red
- Calidad y configuración del equipo servidor
- Calidad de prestadores de infraestructura tecnológica
- Personal responsable de la administración y el mantenimiento de la infraestructura tecnológica

### **Conclusiones:**

- Como resultado de la Auditoria podemos manifestar que se cumplió con evaluar cada uno de los objetivos contenidos en el programa de auditoría.
- El área de sistemas del Colegio Champagnat de Ipiales- Nariño, presenta deficiencias en cuanto a procesos y documentación que permitan un uso óptimo de aplicativo SAPRED para registro y control, que permita tener acceso rápido y fácil a la información a la comunidad educativa .
- No existen políticas de control y documentación en el área de sistemas

- El sistema SAPRED no es explotado en su totalidad por la falta de capacitación a sus diferentes tipos de usuarios, teniendo en cuenta que puede servir de gran apoyo y herramienta fundamental a toda la comunidad educativa.

### **Recomendaciones**

- Realizar una revisión completa de la infraestructura tecnológica tanto a nivel de hardware como de software y garantizar un mejor acceso físico de red
- Actualizar de equipos de red de datos
- Elaborar de manual de funciones para cada puesto de trabajo dentro del área.
- Llevar a cabo socialización permanente a la comunidad educativa en el uso de plataforma tecnológica.
- Socializar acerca de SAPRED con la comunidad educativa en general.

### **Auditoria de Sistemas**

- Elaborar un calendario de mantenimiento de rutina periódica.
- Capacitar al personal.
- Una vez implementados los planes de acción, realizar visita de verificación en seis meses posteriores al inicio de implementación de los mismos.

### **Fecha del Informe**

18 de Enero de 2016

### **Identificación y Firma de los Auditores**

Nelson Adrián Quiroz Chamorro

William Patiño Polanco

### **3.9 INFORME EJECUTIVO DE LA AUDITORÍA**

Ipiales, 18 de Enero de 2016

Señores:  
Directivos  
Colegio Champagnat Ipiales-Nariño  
E.S.M

Cordial saludo.

A continuación presentamos el informe de la auditoría informática aplicada a los procesos del área de sistemas que controlan la parte académica del colegio Champagnat de Ipiales – Nariño durante el periodo comprendido entre octubre de 2015 y Enero de 2016. De antemano agradecemos su completa disposición y colaboración al proceso ejecutado.

Cabe mencionar que la institución posee fortalezas y se destaca positivamente en los siguientes aspectos:

Es una Institución con trascendencia dentro de la ciudad de Ipiales con una amplia y buena infraestructura física de la institución, cuenta con personal calificado y comprometido con las diferentes labores de la institución; además se destaca el manejo de documentación y evidencias de procesos educativos debido a la certificación de calidad ICONTEC ISO 9001, tiene bien definidos los perfiles y guías de cargo de cada uno de los colaboradores. Por otra parte posee un espacio bueno y suficiente para las 2 salas de informática, además de contar con sistemas de información como SAPRED para registro y seguimiento académico. Los docentes poseen un buen uso y apropiación de herramientas TIC. Tiene su respectiva página web institucional dentro de la nube y maneja la administración de documentos en línea como parte del sistema de gestión de calidad

Al momento de iniciar la auditoría se determinaron los siguientes hallazgos:

- Falta de procesos en el área de sistemas para el registro del aplicativo SAPRED, por lo cual se recomienda establecer políticas claras y los dolientes respectivos para cada uno de los procesos del área de sistemas que están vinculados al registro y control del seguimiento académico de los estudiantes.
- Falta control sobre software SAPRED, por lo cual se recomienda establecer los formatos o documentación necesaria para la asistencia y control del software en mención.
- No existe un calendario de mantenimiento SAPRED, por lo cual se recomienda que dentro de la planeación anual se defina un calendario de mantenimiento y

actualización de acuerdo a los requerimientos del PEI, el SIEE u otros que sean de trascendencia e importancia.

- Falta mecanismos de control y comunicación directa con contratista que permita la solución de inconvenientes que refieran al sistema SAPRED, por lo cual se recomienda revisar con detalle los contratos con proveedores, definiendo de forma clara los medios de comunicación, el soporte y la excelente capacitación de los usuarios.
- No existen políticas claras sobre el uso de medios tecnológicos, por lo cual se recomienda establecer claramente las políticas de administración de recursos (verdaderos inventarios, manejo de hojas de vida de los equipos de cómputo, calendarios de mantenimientos preventivos a equipos de cómputo y redes, servicios prestados entre otros)
- No existe un calendario programado de manteniendo de infraestructura tecnológica por lo cual se recomienda que dentro de la planeación, el área de sistemas dentro de su plan de área o plan individual de trabajo establezca su calendario de trabajo en la parte de mantenimiento y se haga seguimiento del plan, al menos 2 veces al año.

Al hacer estas observaciones se recomienda establecer planes de acción inmediatos ya que el área académica juega un papel muy importante en la formación de los estudiantes para el cumplimiento de la misión y visión de la institución.

Por otra parte se recomienda hacer seguimiento de los planes y establecer fecha para una nueva auditoría para evaluar los avances y soluciones establecidas.

Atentamente,

Equipo auditor:

Nelson Adrián Quiroz Ch.

William Patiño Polanco

**Recibido:**

Fecha: \_\_\_\_\_

Nombre: \_\_\_\_\_

Firma: \_\_\_\_\_

## 4. CONCLUSIONES

La ingeniería de sistemas comprende diferentes áreas del conocimiento donde se pueden aplicar las distintas técnicas, métodos y recursos propios de ingeniería para la apropiación de nuevas tecnologías, es así como la rama de la auditoría de sistemas y la seguridad informática se convierte en un ámbito esencial para administrar la información y los recursos de un sistema informático o un sistema de información.

La Auditoría de Sistemas de Información, hoy en día es de vital importancia para las empresas modernas con visión de futuro, sobre todo inmersas en el mundo globalizado, porque si no se prevé los mecanismos de control, seguridad y respaldo de la información dentro de una institución se verá sumida a riesgos lógicos, físicos y humanos, que conlleven a fraudes no solamente económicos sino de información, es decir, pérdidas para la empresa o institución.

Es importante que el colegio Champagnat de Ipiales, siendo una institución certificada por ICONTEC bajo la norma ISO 9001, la cual permite garantizar la calidad de sus servicio, se preocupe y vele también por la calidad y administración de sus sistema de información y sistema informático haciendo ejercicio de las buenas prácticas.

La auditoría estuvo netamente enfocada a los procesos del área de sistemas que controlan la parte académica del colegio Champagnat de Ipiales-Nariño, sin embargo se hace evidente también la necesidad de una auditoría a los procesos que controlan las otras áreas de la institución.

El desarrollo de la auditoría se debió entre otras cosas al dominio y conocimiento integral de los procesos que afectan la planeación de procesos y la seguridad informática de la información con vulnerabilidades, amenazas y riesgos en el colegio Champagnat de Ipiales- Nariño.

La auditoría se planificó y desarrolló bajo el estándar COBIT con el cual se realizó la selección de dominios y procesos de acuerdo a los hallazgos determinados previamente en la recolección y análisis de la información; seguidamente se hace el análisis de los objetivos de control enfocando en aquellos que presentaba mayor nivel de riesgo; y con base en esto se procede a instaurar los posibles planes de acción. Se detalla un informe de auditoría en el cual se presentan los dominios, procesos y objetivos de control trabajados, las recomendaciones pertinentes y las conclusiones del plan de auditoría.

## **5. RECOMENDACIONES**

Realizar auditorías informáticas constantes para evaluar los procesos del área de sistemas, así como también al personal y documentación que administran la parte académica del Colegio Champagnat de Ipiales –Nariño.

Realizar diagnósticos permanentes de la forma como se administran los procesos y la documentación del área de sistemas.

Planear, diseñar y ejecutar instrumentos y pruebas que permitan determinar las causas de los problemas más frecuentes del área de sistemas.

Presentar un informe final de los hallazgos de la auditoría y las respectivas recomendaciones y posibles soluciones a la problemática encontrada.

Aplicar las recomendaciones realizadas y llevar a cabo seguimiento de los planes de acción.

## BIBLIOGRAFIA

CAICEDO, Liliana. ORDONEZ, Claudia. Técnicas de Auditoria de Sistemas Aplicadas al Proceso de Contratación y Páginas Web en Entidades Oficiales del Departamento de Nariño. Universidad de Nariño. 2010.

EXPANSIÓN, *Control Interno, Auditoría y Seguridad Informática. Tomos II-IV*, 1996.

HERNÁNDEZ HERNÁNDEZ, Enrique. *Auditoría en Informática. Un enfoque metodológico y práctico*. CECSA. México, 1999

PIATTINI, Mario G; Del Peso, Emilio, *Auditoría Informática. Un enfoque práctico*. Rama. Madrid, 1998

SOLARTE, Francisco Nicolás, GUSTÍN Enith, HERNANDEZ Ricardo. Manual De Procedimientos para Llevar a la Práctica La Auditoría Informática y de Sistemas, IUCESMAG, Pasto, 2013.

## NETGRAFIA

- <http://auditordesistemas.blogspot.com.co>
- <http://www.isacabogota.net/metodologias/cobit.aspx>
- <http://es.wikipedia.org/wiki/COBIT>
- <http://www.network-sec.com>
- <http://www.normas9000.com>
- <http://www.monografias.com>
- <http://www.parquesoftpasto.com>
- <http://www.serviciostic.com>
- <http://www.sccc.co.cl>

# **ANEXOS**