AUDITORIA INFORMÁTICA A LA INFRAESTRUCTURA TECNOLÓGICA Y SISTEMAS DE INFORMACIÓN BAJO EL ESTÁNDAR COBIT EN LA INSTITUCIÓN EDUCATIVA ESCUELA NORMAL SUPERIOR DE QUIBDÓ

BETTY JANETH MACHADO LLOREDA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
QUIBDÓ
2018

AUDITORIA INFORMÁTICA A LA INFRAESTRUCTURA TECNOLÓGICA Y SISTEMAS DE INFORMACIÓN BAJO EL ESTÁNDAR COBIT EN LA INSTITUCIÓN EDUCATIVA ESCUELA NORMAL SUPERIOR DE QUIBDÓ

BETTY JANETH MACHADO LLOREDA

Asesor del Proyecto
HERNANDO JOSÉ PEÑA HIDALGO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
QUIBDÓ
2018

CONTENIDO

LISTA DE CUADROS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág

1. TITULO

AUDITORIA INFORMÁTICA A LA INFRAESTRUCTURA TECNOLÓGICA Y SISTEMA DE INFORMACIÓN BAJO EL ESTÁNDAR COBIT EN LA INSTITUCIÓN EDUCATIVA ESCUELA NORMAL SUPERIOR DE QUIBDÓ

2. INTRODUCCIÓN

La auditoría desde hace muchos años nació con el objetivo de evitar fraudes en las empresas, se consideraba perteneciente a las áreas administrativas, luego se propagó a otras áreas, como las ingenierías, medicina y sistemas; solo se encargaba de observar registros.

La auditoría de sistemas se encarga de realizar a la verificación para conocer si los sistemas funcionan correctamente y cumplen con el objetivo para el cual se diseñaron, se evalúa también, el conjunto de planes y políticas, de igual forma las actividades que se desarrollan dentro del mismo.

Debido a las fallas informáticas que se han venido presentando desde hace muchos años, se vio la necesidad de realizar inversiones para proteger la seguridad informática de las empresas; muchas organizaciones no le prestaban atención a la seguridad de sus sistemas, al pasar los años se ha visto la necesidad de proteger los activos informático, debido las diferentes riesgos a los que se ven expuestos, por avance de técnicas de ataques y la vulnerabilidad, los cuales han conllevado a ser blancos de: revelación de información confidencial, fallas, daños tanto en el hardware como en el software, robos, entre otros; generándoles grandes pérdidas.

La Auditoría Informática consiste en verificar, analizar y evaluar como una organización utiliza sus recursos informáticos y el flujo de información, como los protege y de qué forma realiza el control y seguimiento de sus servicios, así mismo, busca identificar si existe trazabilidad en sus actividades, si cumplen adecuadamente con los fines de la organización, la normatividad y demás regulaciones.

En el presente proyecto se realizará la auditoria al Sistema de Información y a la infraestructura tecnología de la escuela normal Superior de Quibdó, se tendrá una evaluación real de la situación de seguridad de dicha institución, realizaran recomendaciones para acciones de mejora continua en materia de seguridad, de tal manera que los directivos de la Institución Educativa, se pueda dar cuenta del impacto financiero, perdida de información y daños de los implementos físicos, que se presentan por tener los sistemas expuestos a incursiones y ataques, lo mismo permitirá establecer controles de seguridad y protección.

3. DEFINICIÓN DEL PROBLEMA

La Escuela Normal Superior de Quibdó, es una institución educativa de carácter oficial; tiene su sistema de información e infraestructura tecnológica expuestos a la incursión de cualquier ataque; sea por virus, troyanos o hacker, hay muchos usuarios para el acceso al sistema y acceden a este desde cualquier sitio sin tener las precauciones necesarias. La falta de control y capacitación de los usuarios que acceden a la sala de informática, la falta de seguridad de la misma, el uso indebido de los recursos y la falta apropiación en materia de administración de los mismos, afectan el buen funcionamiento de los medios informáticos.

A pesar de esta problemática, las directivas de esta institución desconocen el impacto que genera esta situación en la organización lo que facilita que este tipo de riesgos aumenten cada día.

Como resultado de esta falencia se presentan en el aula informática: violación de la intimidad de la información, uso inadecuado, incursiones de virus, perdida de información y daño al hardware.

¿Cómo la auditoria informática a la infraestructura tecnológica y sistemas de información, permitirá realizar una evaluación para verificar la seguridad informática en la Institución Educativa de la Escuela Normal Superior de Quibdó?

4. JUSTIFICACIÓN

La realización del proyecto es importante debido a que permite evaluar la eficiencia en seguridad informática y establecer controles de mejora, medir el impacto financiero que genera la falta de seguridad en los medios informáticos.

Mediante la auditoria al Sistema de Información y a la infraestructura tecnología de la escuela normal Superior de Quibdó se tendrá una evaluación real de la situación de seguridad de dicha institución y se podrá establecer recomendaciones para mejorar los niveles de seguridad al interior de la institución, garantizando la seguridad de la información que se maneja; de tal manera que los directivos de la Institución Educativa, se pueda dar cuenta del impacto que se genera al tener los sistemas expuestos a incursiones y ataques, así como establecer controles de seguridad y protección.

5. OBJETIVOS

5.1 OBJETIVO GENERAL

Realizar la evaluación de la seguridad informática aplicando procesos de auditoría a la infraestructura tecnológica y sistemas de información en la Institución Educativa Escuela Normal Superior de Quibdó.

5.2 OBJETIVOS ESPECÍFICOS

1. Elaborar un inventario de los activos informáticos de la Escuela Normal Superior de Quibdó.

2. Realizar un diagnóstico del problema de seguridad de los elementos informáticos de la IE Escuela Normal Superior de Quibdó.

3. Realizar un análisis que permita la gestión de riesgos encontrados.

4. Proponer a la IE Escuela Normal Superior de Quibdó acciones de mejora que coadyuve con la gestión de riesgos y al mejoramiento de su seguridad.

6. MARCO REFERENCIAL

6.1 ANTECEDENTES

- El proyecto denominado “CALIDAD Y SEGURIDAD DE LA INFORMACIÓN Y AUDITORÍA INFORMÁTICA”, presentado por Esmeralda Guindel Sánchez, en UNIVERSIDAD CARLOS III DE MADRID, explica los procesos de auditoria, concepto y campo de aplicación, se tendrá en cuenta para realizar la fundamentación teórica del proyecto.

- La Ponencia “AUDITORIA EN SEGURIDAD INFORMÁTICA”, presentada por JHON EDINSO MARTINEZ Y CARLOS ANDRES GIRALDO; explica el concepto de auditoría informática, los aspectos que se deben tener en cuenta para llevar a cabo el proceso de auditoría, lo cual permite tener una evaluación precisa para darse cuenta si sus sistemas son totalmente seguros o no. Se usará como componente de sustentación teórica y análisis de técnicas de auditoria.

- El artículo “AUDITORÍA Y SEGURIDAD DE SISTEMAS DE INFORMACIÓN”, presentado por Luis Elissondo, habla sobre el concepto de COBIT y la relación con auditoria en seguridad informática y como implementarla. Se tomará para el proceso de implementación de la auditoria con el estándar COBIT.

- La Tesis myEchelon: Un sistema de Auditoría de Seguridad Informática Avanzado bajo GNU/Linux, presentado por Jiménez Alberto y Gómez Julio; Tesis sobre auditoría en seguridad Informática, se tendrá en cuenta para el concepto de auditoría en seguridad informática, como se realiza y los estándares para realizar auditoria en seguridad informática.

6.2 MARCO CONTEXTUAL DE LA EMPRESA

La Institución de Educativa Escuela Normal Superior de Quibdó, presta servicios educativos de carácter oficial:

> Fue creada en el gobierno del doctor Alfonso López Pumarejo en 1936 y su gestor fue el Doctor Diego Luis Córdoba. Inicio sus labores en la casona adyacente a la

catedral de Quibdó. Su himno fue compuesto por el doctor Armando Torres, quien fue estudiante, docente, vicerrector, y finalmente, su rector. El estudio fue diseñado por el doctor Oscar Serna, egresado de la institución y ex gobernador del choco. Ha expedido los títulos de maestro, maestro superior, bachiller pedagógico y normalista superior a miles de chocoanos quienes a lo largo y ancho del país educan a la población colombiana. Muchos han incursionado en la política y ocupado altas dignidades: gobernadores, procuradores regionales, contralores departamentales, alcaldes, entre otros. El terreno donde está actualmente constituido el edificio fue donado por los señores Juan Garcés, Juan Bautista y Francisco Córdoba y tiene un área de 114.000m[21].

- **MISIÓN:** "La Escuela Normal Superior De Quibdó, tiene como misión prestar el servicio educativo dentro de los cánones de la calidad y la inclusión en los niveles de preescolar y el ciclo de básica primaria, con competencias académicas, pedagógicas, ciudadanas, ambientales y tecnológicas en la información que le permita un desempeño eficiente en contexto."[2]

- **VISIÓN:** "La escuela normal superior de Quibdó se visiona hasta 2019 como una institución líder en el campo de la educación que valora la pedagogía como la disciplina que orienta su quehacer educativo en la formación de maestros superiores a través de la didáctica, la investigación, la educación ambiental y el uso racional de las tecnologías de la información y la comunicación"[3].

La institución Educativa Escuela Normal Superior de Quibdó actualmente cuenta con un sistema de información SI3 para el tratamiento de estudiantes y notas, manejado desde 3 computadores con acceso a la plataforma desde los navegadores mozilla y google chrome:

- Ingreso de Estudiantes - Secretaria.
- Notas y Certificados – Área Administrativa

---

[1] ARBOLEDA, Nicolas Ibarguen. 2012**.** Reseña Historica de lLa E.N.S.Q. [En línea]. Jun. 2012 [Citado el: 30 de 08 de 2014]. Disponible en internet: < URL: http://escuelanormalquibdo.blogspot.com.co/>

[2] ESCUELA NORMAL SUPERIOR DE QUIBDÓ. Portal Institucional. [En línea] [Citado el: 30 de 08 de 2015.]. Disponible e Disponible en internet: < URL: http://ienormalquibdo.edu.co/portal/>

[3] Ibíp.

- Autorizaciones de Claves de Acceso para docentes – Coordinación Académica.
- Carnetización.
- Información de estudiantes y docentes.
- Sistema de información colectiva.
- Egresados.

Cuenta además con una sala de informática de 50 equipos portátiles del programa computadores para educar, el sistema operativo Windows 8, donde los estudiantes se capacitan en cursos desde primero hasta el ciclo complementario, a su vez ingresan a plataforma para obtener información de pruebas pisa y saber.

6.3 MARCO TEÓRICO

A medida que los sistemas avanzan también existen personas que quieren atacar los sistemas informáticos aprovechando las vulnerabilidades de dichos sistemas, no solo con el hardware o software, sino también con todos los elementos que intervienen. A diario se observa como muchas entidades de orden mundial les ha ocasionado pérdidas millonarias tanto en información como en dinero porque su información confidencial es revelada o sus sistemas atacados, se observa diferentes tipos de ataques a través de virus, troyanos, intrusos, hackers, con fines delictivos son una realidad donde nadie se escapa, porque los sistemas no son totalmente seguros. A continuación, se describen algunos aspectos relacionados con el proyecto

6.3.1 Auditoria de Sistemas

Es el proceso de evaluación de los sistemas de información dentro de una empresa para verificar los controles de procesamiento de información, permite observar si los sistemas son efectivos y pueden apoyar al logro del objetivo de la misma; se puede asegurar que los datos sean verídicos; garantizar la seguridad de la información, del personal y de las instalaciones; minimizar los riesgos, permite además conocer la situación informática de la empresa. El establecimiento de controles físicos y lógicos, los cuales ayudan a brindar soporte a los directivos, como también la búsqueda de los controles administrativos que ayuden a la toma de decisiones.

6.3.2 Auditoria Informática

Evalúa los equipos computacionales, el tratamiento de la información, el hardware, el software y los centros de procesamiento, lo que permite establecer controles técnicos, para garantizar el uso adecuado de los medios informáticos. La Auditoría Informática es importante para las empresas porque se puede verificar, analizar y evaluar como ellas utilizan sus recursos informáticos, como los protegen y de qué forma realiza el control y seguimiento de sus servicios, pueden además identificar si se están llevando acabo los procedimientos necesarios en sus actividades, si los activos informáticos cumplen adecuadamente con los objetivos de la organización y demás aspectos relacionados con ella y a su vez observar si los sistemas como procesos informáticos funcionan adecuadamente y sus activos se encuentren debidamente protegidos.

Dentro de los objetivos de auditoría Informática están:

- Analizar la eficiencia de los sistemas, los procesos y controles informáticos.
- Examinar si los medios informáticos al igual que los sistemas cumplen con las normas pertinentes.
- Verificar la gestión la infraestructura informática y recursos del Hardware, redes, Sistemas eléctricos, niveles de seguridad, Software, Desarrollo de sistemas y Procesamiento de datos.
- Evaluar las responsabilidades del personal interviniente en todos los procesos informáticos.
- Estimar como se identifican, administran y se gestionan los riesgos informáticos.
- Evaluar la inversión que se realiza en seguridad informática.
- Establecer planes de contingencia y medidas

6.3.4 Auditoria en Seguridad Informática

Encargada de realizar la verificación para que los sistemas funcionen correctamente y cumplan con el objetivo para el cual se diseñó, lo mismo que para detectar errores y fallas. Permite evaluar si se está cumpliendo con la confidencialidad, integridad y disponibilidad de la información.

6.3.5 Metodología de para la realización de la auditoría

Se realiza la auditoria en 3 fases:

- **Fase de Planificación:** Se establecen el área dentro de la empresa que será auditada, el alcance, los objetivos, procesos y procedimientos de la misma, para ofrecer resultados de acuerdo con las políticas y objetivos. Elaboración de presupuestos, asignación de recursos físicos y tecnológicos, definición de actividades que se van a realizar dentro del proceso.

- **Fase de Ejecución:** Después de la planeación se ejecuta la auditoria siguiendo los pasos y procedimientos establecidos para que se lleve a feliz término.

- **Fase de Resultados:** se realiza el informe final de la auditoria con los hallazgos encontrados en el proceso, se emite el dictamen final.

Existen varios estándares para realizar la auditoria en seguridad informática dentro de los cuales están:

- COBIT (objetivos de Control de la Tecnológica de la Información)
- Normas ISO 17799, 27001 y 27002
- Normas NFPA75
- TIA 942
- ISACA

6.3.6 Análisis de Riesgos

El análisis de riesgos comprende la utilización de la información disponible mediante la cual se pretende identificar cada uno de los peligros a los que se está expuesta la empresa, en la gestión de riesgos es necesario tener claro los siguientes conceptos:

1. Amenazas: Causa potencial de un daño a un activo.

2. Vulnerabilidad: Debilidad de un activo que puede ser aprovechado por una amenaza.

3. Impacto: Consecuencia de que la amenaza ocurra.

4. Riesgos intrínsecos: Calculo del daño probable a un activo si se encontrara desprotegido.

5. Salvaguardas o controles: medidas que ayudan a minimizar el riesgo.

6. Riesgos residuales: riesgos que quedan tras la aplicación de salvaguardas o controles.

7. Teniendo en cuenta que metodología se va a implementar en una organización, se debe realizar un buen análisis y medición de los riesgos a los que se exponen, se debe tener en cuenta los siguientes aspectos:

- Ayudar a los responsables de las organizaciones de información para que se conozca la existencia de riesgos y la necesidad de gestionarlos, Ofrecer una metodología para analizar los riesgos.

- Ayudar mediante la metodología para el tratamiento oportuno de los riesgos.

- Dar soporte a la organización para realizar una buena gestión de riesgos (Análisis y Tratamiento).

Para lograr proteger la organización ante los posibles riesgos que pueden poner en peligro la seguridad de la empresa, es necesario realizar un buen análisis e identificación de los mismos, lo cual ayuda a que se puedan tomar medidas para lograr minimizarlos, dentro de las pueden ser:

- Hacer restauración o copias de respaldo, para una vez ser atacado tener los respaldos para continuar en los sistemas.

- Capacitar por dependencias de acuerdo a las funciones del personal sobre los objetivos y los procedimientos que enmarcan a la empresa y las acciones a tomar ante posibles riesgos.

- Clasificación de las responsabilidades y del personal idóneo para acceder a informaciones críticas de la empresa.

- Implementación de un sistema de detección de intrusos habilidosos como los hackers.

6.3.6.1 Metodología de Análisis y Evaluación de Riesgos

Existen varias metodologías de tratamiento de riesgos dentro, de las cuales está la metodología Magerit, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, la cual se pretende concientizar a la empresa de los riesgos que corre y la forma de cómo se pueden tratar de tal manera que no genere un impacto negativo a la empresa. Se requiere adelantar algunos pasos fundamentales:

1. Definición de Activos: Siempre es necesario para realizar un análisis de riesgos, conocer sus activos, partiendo de un grupo que sea relevante y manejable, cada uno de esos activos deberán tener sus amenazas, las vulnerabilidades y el impacto con el que se puede analizar cada uno de los riesgos.

2. Amenazas: Son las causas potenciales que pueden generar daño en los activos, son factores externos que no se pueden controlar.

3. Vulnerabilidades: Las vulnerabilidades son las exposiciones de los activos para recibir cualquier tipo de ataque, comprometiendo así la Confidencialidad, integridad y disponibilidad, por lo que se requiere identificar las debilidades que se tiene y clasificarlas de acuerdo a una escala.

4. Salvaguardas: Las salvaguardas son todos los mecanismos o controles que se deben llevar a cabo para reducir los riesgos.

6.3.6.2 Estimación del Riesgo

La estimación o medición del riesgo es el grado de peligrosidad de los mismos, también se puede considerar como el impacto que genera dentro de la organización si el riesgo llegara a ocurrir, en el cuadro siguiente se toman escalas cuantitativas y cualitativas para su medición.

Cuadro 1. Escalas cualitativas y cuantitativas

Impacto	Probabilidad	Riesgo
C: Catastrófico (3)	A: Alta (3)	A: Alto
M: Moderado(2)	M: Media (2)	M: Medio
L: Leve (1)	B: Baja (1)	B: Bajo
Fuente Solarte Francisco. Auditoría Informática y de Sistemas		

Cuadro 2. Rango de Estimación del Riesgo

Rango Inferior	Nivel del Riesgo	Rango Superior
0>=	B: Bajo	<=3
3>=	M: Medio	<=6
6>=	A: Alto	<=9
Fuente Solarte Francisco. Auditoría Informática y de Sistemas		

Es necesario calcular nivel del riesgo, para ello se requiere analizar los siguientes conceptos: el impacto y la probabilidad del riesgo; cuando se refiere al impacto se considera el nivel del daño que este puede generar si ocurre y la probabilidad consiste en analizar conque frecuencia el que ocurre el riesgo, en el siguiente cuadro se tomara el cálculo del Nivel del Riesgo.

Cuadro 3. Cálculo del Nivel de Riesgo

Riesgos		Probabilidad		
		A: Alta(3)	M: Media (2)	B: Baja (1)
Impacto	C: Catastrófico (3)	A=9	M=6	B=3
	M: Moderado(2)	M=6	M=4	B=2
	L: Leve (1)	B=3	B=2	B=1
Fuente Solarte Francisco. Auditoría Informática y de Sistemas				

6.3.7 COBIT (Objetivos de Control para Información y Tecnología)

Es una guía de ISACA, para controlar y supervisar la tecnología de la información; debido a sus amplios servicios, tiene recursos que le pueden servir a cualquier entidad pública o privada, para ser usado como de marco de referencia de la gestión de TI. Las entidades que quieran implementar su gestión de TI con COBIT, este estándar les ofrece: un resumen ejecutivo, un módulo, objetivos de control, mapas de auditoría, herramientas para su implementación y la una guía de técnicas de gestión.

Teniendo en cuenta que en la actualidad la información juega un papel muy importante en cualquier empresa pública o privada, el uso del Marco referencial COBIT ayuda a alcanzar los objetivos, además de reducir riesgos que se presentan actualmente por no tener estandarizados sus recursos tecnológicos con los procesos de la organización, lo que puede con llevar a que se dupliquen los procesos perdiendo eficacia y eficiencia en los mismos; las TI deben proporcionar mejora en los procesos y no ocasionar dificultad en el desarrollo de las actividades. Dentro de los beneficios que ofrece el marco COBIT se puede mencionar:

- Permite soportar las decisiones mediante el mantenimiento de información de alta calidad.

- Se obtiene beneficios haciendo uso efectivo e innovador de TI, para alcanzar los objetivos estratégicos.

- Se logra mantener los riesgos relacionados con TI a un nivel aceptable, dando así eficiencia y eficacia a la organización.

- Hace que se optimice costo de servicios de TI.

- Es un apoyo el cumplimiento normativas y políticas.

- Optimiza los servicios del consto de las tecnologías de información, al igual que la gestión de nuevas tecnologías.

Con la implementación de COBIT se realizan requerimientos de información del negocio los cuales son:

- **La efectividad:** información que se proporciona oportuna, veraz que se puede utilizar en el negocio siendo importante y pertinente.

- **La eficiencia:** la información llegue haciendo un uso óptimo de los recursos.

- **La confidencialidad:** la información solo sea visible por el personal autorizado.

- **La integridad:** la información solo sea modificada por el personal autorizado en la empresa.

- **La disponibilidad:** la información esté disponible y a tiempo cuando sea requerida en cualquier momento.

- **El cumplimiento**: Establecimiento de políticas internas y externas para acatar las leyes inmersas en las actividades del negocio.

- **La confiabilidad:** información apropiada que ayude a la toma de decisiones a la alta gerencia.

COBIT está dividido en:

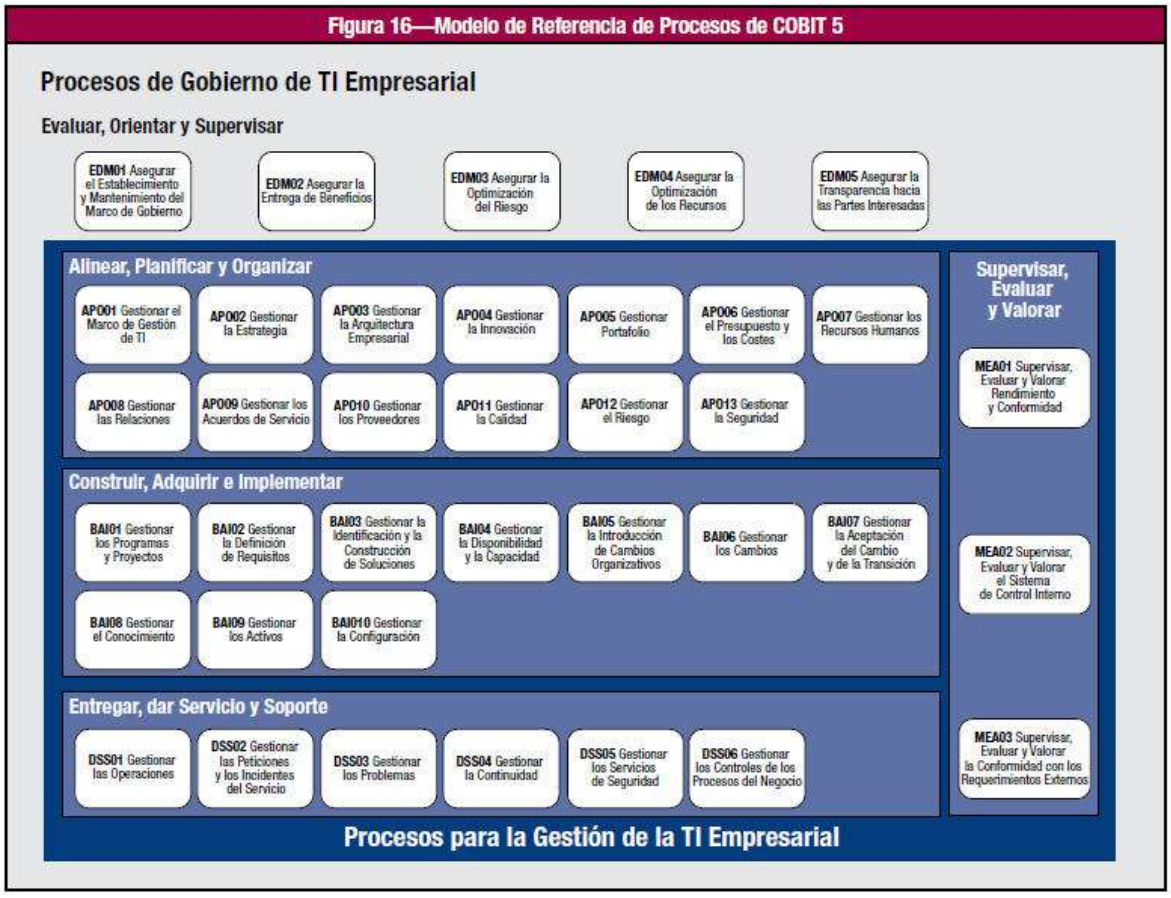
- Dominios: Es una agrupación de procesos con una responsabilidad dentro de la organización.

- Procesos: Conjuntos de actividades.

- Actividades: Acciones para lograr un resultado.

- Tiene procesos agrupados en dominios como lo muestra la siguiente imagen:

Figura 1**:** Dominios y Procesos COBIT



Fuente: ISACA-COBIT 5, 2012

La mayor prioridad para las organizaciones en el trascurso de los años, es mantener la seguridad informática, la cual ayuda a mejorar la prestación de servicios, implementando políticas, procedimientos y métodos, para mantener la confidencialidad, integridad y disponibilidad de la información, garantizando que mantenga segura. Debido a ello es necesario establecer Sistemas de Gestión de Seguridad Informática para tener claros lineamientos, políticas, normas, procesos, que ayudaran a manejar, controlar e implementarlos; para garantizar un correcto funcionamiento de la seguridad informática, pero todo esto se logra con el apoyo constante de la alta gerencia, lo que ayuda a incentivar a los involucrados al buen manejo y aplicación de los sistemas para contrarrestar la vulnerabilidad de la información.

Dentro del mismo es necesario realizar el proceso de la identificación de riesgos, para poder tratarlos y gestionarlos de tal manera que no genere un impacto negativo para la organización, para ello se debe tener una metodología clara para gestión de los tipos de riesgos que se puedan presentar en materia de seguridad, la auditoría permite realizar evaluación de los sistemas que le permitan minimizar los riesgos.

La seguridad informática, toma cada vez más fuerza, en la sociedad de la era digital son muchos los aspectos que se deben tener en cuenta para el buen funcionamiento y desarrollo de los sistemas, debido a que por la injerencia que tiene el hombre frente a éstos, son blanco fácil de cualquier manipulación, abuso y uso ilegal, los ataques informáticos a los que se ven expuestas las organizaciones y entidades, todo esto ocurre a medida que los sistemas avanzan, ya que también avanzan las técnicas y métodos de ataques, aprovechando las vulnerabilidades de los sistemas, en los cuales se ven involucrados el personal de la empresa; por medio de la auditoria informática se permite dar cuenta si la entidad es vulnerable a cualquier ataque que pueda afectar la confidencialidad, la integridad y la disponibilidad de la información. El proyecto de auditoria en seguridad informática busca consolidar una propuesta de investigación para tratar temas de seguridad en un entorno empresarial o de orden social.

6.4 MARCO CONCEPTUAL

Seguridad de información: Se encarga de proteger, la confidencialidad, integridad y disponibilidad de la información en una organización y que sea usada para los fines que se definió y para acceder o modificar dicha información sea por el personal autorizado.

Confidencialidad: Se encarga de que la información sea visible solo por el personal autorizado.

Disponibilidad: Que la información este en todo momento y lugar, fácil acceso a ella por el personal autorizado.

Integridad: garantiza que la información solo sea modificada por el personal autorizado.

No Repudio: Garantiza que el receptor no niegue que recibió la información.

Estándar: Conjunto de normas nacionales e internacionales que regulan la seguridad de la información.

Modelos de seguridad informática: Esquemas o patrón a seguir donde que establecen las políticas de la seguridad de la información, éste puede ser reproducido o imitado

Riesgo: es la posibilidad que exista algo que afecta el desarrollo del proyecto sea positivo o negativo.

Hardware: la estructura física del sistema informático incluye computadores, elementos de la red, servidores, tarjetas de red.

Software: es lo intangible, el conjunto de programas, los Sistemas Operativos, las aplicaciones.

La Información: es el activo principal y comprende el conjunto de dato lógicos que procesa el software, corresponde a lo que está en la base de datos, los datos de la intranet, la información de usuarios, la información bien organizada de la empresa.

Los usuarios: son las personas que intervienen en el sistema de información: Administrador de la red, técnicos, encargado de seguridad.

6.5 MARCO LEGAL

- **Decreto 1151 del Ministerio de Comunicaciones,** mediante el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.

- **Ley 1341 de 30 de julio de 2009,** sobre principios y conceptos sobre la Sociedad de la Información y la Organización de las Tecnologías de la Información y las Comunicaciones.

- **Ley 1273 de 2009**, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

7. DISEÑO METODOLÓGICO

7.1. POBLACIÓN

Institución Educativa Escuela Normal Superior de Quibdó ubicada en el casco urbano de la ciudad de Quibdó departamento del Chocó, cuenta con 6 sedes, tiene 2867 estudiantes, 150 docentes y 12 personal administrativo.

7.2. MUESTRA

Los docentes y directivos docentes que intervienen en el Sistema de Información, responsables de la sala de informática al igual que una muestra de 30 estudiantes de los grados decimo y once de la Institución, equivalentes al 15 % del total de los estudiantes de los grados citados.

7.3 TIPO DE INVESTIGACIÓN

Explicativa debido a que se explicará mediante el estándar COBIT, los riesgos, las vulnerabilidades y amenazas que existen en el Sistema de Información y en la infraestructura tecnológica de la IE Escuela Normal Superior de Quibdó.

7.4 INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

- **Entrevistas:** Se usarán para conocer la percepción de las de las directivas sobre la seguridad informática.

- **Observación**: Se observará los elementos a ser auditados, para reconocer la importancia para que se realice la auditoria en la institución.

- **Listas de Chequeo:** Se utilizará para saber si el objetivo de la auditoria se está cumpliendo, tener claro el paso a paso a seguir y que falta para la implementación del proyecto.

7.5 METODOLOGÍA DE DESARROLLO

Se llevará cabo mediante las 4 fases de la Auditoria:

1. **Conocer el área auditada:** se determinará el área auditada mediante entrevistas y observación.

2. **Planear la auditoría:** Elaboración del plan estratégico con los pasos que se llevaran a cabo durante el proceso de auditoria teniendo en cuenta el estándar COBIT.

3. **Ejecutar la Auditoria:** una vez elaborado el plan estratégico, se llevará a cabo la ejecución de la auditoria, identificación de activos para la gestión de riesgos, se aplicará las listas de chequeo por cada objetivo de control de Cobit seleccionados para la auditoria.

4. **Fase de resultados:** se elaborará el dictamen de la auditoria teniendo en cuenta lo arrojado en la etapa de ejecución de la misma.

Objetivo 1: Elaborar un inventario de los activos informáticos de la Escuela Normal Superior de Quibdó.

Actividades:

- Realización de entrevistas con las directivas de la IE.

- Visitas para conocer el sistema de información.

Objetivo 2: Realizar un diagnóstico del problema de seguridad de los elementos informáticos de la IE Escuela Normal Superior de Quibdó, que permita establecer una ruta de mejoramiento.

Actividades:

- Elaboración del plan estratégico con los pasos que se llevaran a cabo durante el proceso de auditoria teniendo en cuenta el estándar COBIT.

Objetivo 3: Realizar un análisis que permita la gestión de riesgos encontrados.

Actividades:

- Identificación de Activos y riesgos.

- Revisión del Sistema de Información.

- Revisión de la infraestructura tecnológica.

Objetivo 4: Proponer a la IE Escuela Normal Superior de Quibdó acciones de mejora que coadyuve con la gestión de riesgos y el mejoramiento de su seguridad.

Actividades:

- Elaboración del documento final con los resultados arrojados en la auditoria.

- Presentar el dictamen a las directivas de la IE.

- Elaborar propuestas acciones preventivas y de mejora.

8. DESARROLLO DEL PROYECTO

8.1 ELEMENTOS QUE SERÁN AUDITADOS

Para dar cumplimiento al objetivo 1**:** Elaborar un inventario de los activos informáticos de la Escuela Normal Superior de Quibdó.

Entrevistas con las directivas de la IE: Se realizó la visita a la Institución Educativa Escuela Normal Superior de Quibdó para realizar la entrevista al rector del establecimiento educativo El Especialista Efraín García Serna para conocer las áreas que serán auditadas, su funcionando y la identificación de activos.

El área de informática de la institución, está compuesta por una sala de 50 computadores portátiles, para dictar clases a los estudiantes de la institución, y proyección comunitaria y diversas tareas desarrolladas por los docentes dentro de la institución, en la figura 1 se muestra la estructura física de la sala.

Figura 2. Instalaciones del Aula de Informática

Fuente: El Autor

Los docentes quienes dictan informática en la institución son quienes garantizan el acceso a los estudiantes, pese a que no existe una estructura organizacional definida, se detallas las funciones que realiza cada uno:

- El coordinador: el docente encargado del aula informática, realiza la planeación de los horarios para la utilización de la sala, la administración de los recursos informáticos y de personal.

- Docentes de apoyo: son dos docentes que se encargan de dictar clases de informáticas a los estudiantes y apoyo a los compañeros en la utilización de los recursos informáticos en el aula.

- Soporte Técnico: en esta área se encarga de brindar soporte técnico a los computadores, a los implementos de hardware y redes, mantenimiento correctivo y preventivo; configuración de periféricos, actualización de sistema, esta área se apoya con practicantes del SENA.

Visitas para conocer el sistema de información: La institución cuenta con un portal institucional diseñado por la empresa "Mundo de Soluciones Efectivas S.A.S." Este sistema es de información colectiva donde se encuentra la información de la institución como lo son: Misión, Visión, PEI, proyectos manejados, acceso sistema de notas S3, servicio de correo electrónico, sistema de votación electrónica, red social y para el seguimiento a los egresados, como se visualiza en la figura 2.

Figura 3. Portal Institucional

Fuente: http://ienormalquibdo.edu.co/portal/

El Sistema de Información denominado ***Sistema Integrado de Información Institucional (SI3)*** para la gestión de todos los procesos académicos de la institución, con acceso a la plataforma desde los navegadores mozilla y google Chrome, por medio de este sistema se realizan los siguientes procesos:

- Ingreso de Estudiantes.
- Notas y Certificados
- Autorizaciones de Claves de Acceso para docentes
- Certificaciones.
- Carnetización.
- Información de estudiantes y docentes.
- Seguimiento a Egresados

En la figura 2 se muestra la página de inicio de al Sistema Integrado de Información:

Figura 4. Pagina de Acceso SI3

Fuente: http://ienormal.mundosoluciones.com.co/si3/login/

El operador del sistema es quien brinda el soporte técnico, capacita a la institución en el manejo del SI3, también brinda las asesorías técnicas ante fallas del sistema. La Institución solo hace el cargue de la información al sistema, cuenta con los siguientes perfiles de acceso:

Rector: Tiene el manejo de toda la información de la institución.

Secretaria: Se encarga de realizar procesos de matrículas, expedición de certificados, retiro de estudiantes.

Coordinación Académica: Administra todos los procesos académicos, configuración del sistema para el registro de notas, concede permisos a los docentes para ingreso de notas, también concede permisos especiales, gestiona las claves de acceso a los docentes y estudiantes, carga académica de los docentes, carga de los directores de grupo, seguimiento a la planilla de notas, emisión de alertas en caso de novedades.

Docentes: Se encargan del registro de las notas en los tiempos que la coordinación académica lo habilite, modifica nota a los estudiantes para ello es necesario que el coordinador le conceda un permiso especial para poder hacerlo.

Estudiantes: Visualizar los datos de sus notas correspondiente al año

Elementos a Auditar

- **Sala de informática de la institución:** De la sala se auditará la gestión administrativa de la sala de cómputo, cumplimiento de las funciones y prestación de servicios, infraestructura física, seguridad física, ubicación, infraestructura eléctrica y redes.

- **Portal Institucional:** Gestión y actualización de la información.

- **Sistema SI3**: Usuarios que acceden al sistema y utilización de la información.

8.2 PLAN DE AUDITORIA

Objetivo 2: Realizar un diagnóstico del problema de seguridad de los elementos informáticos de la IE Escuela Normal Superior de Quibdó, que permita establecer una ruta de mejoramiento.

Actividades: Elaboración del plan estratégico con los pasos que se llevaran a cabo durante el proceso de auditoria teniendo en cuenta el estándar COBIT.

El Plan Estratégico Contiene las actividades que se van a desarrollar en el proceso de auditoría, los responsables, fechas y recursos necesarios para la misma.

Objetivo de la Auditoria

Evaluar la seguridad informática de la infraestructura tecnológica y sistemas de información en la Institución Educativa Escuela Normal Superior de Quibdó.

Alcance

Se evaluará la gestión administrativa de la sala de cómputo, cumplimiento de las funciones y prestación de servicios, infraestructura física, seguridad física, ubicación, infraestructura eléctrica, redes, Gestión y actualización de la información, Usuarios que acceden al sistema, utilización de la información.

Identificación de Recursos para la Auditoria

En el proceso de auditoria se utilizarán los siguientes recursos:

- **Recursos Humanos:** Será realizada por profesional en Ingeniería de sistemas, Estudiante de Especialización en seguridad Informática.

- **Recursos Físicos:** Instalaciones de la Escuela Normal Superior de Quibdó.

- **Recursos Auxiliares:** Resma de papel, fotocopias, tonner.

- **Recursos Tecnológicos:** Computador Portátil, CD, Memorias USB

Plan Con Actividades Propuestas: En el siguiente cuadro se detallan las actividades a realizar en el proceso de auditoria

Cuadro 4: Actividades a Realizar

Actividades	**Fecha**	**Materiales**
Elaboración de Cuestionarios	14/04/2016	Portátil
Visitas a la Institución para tener conocimiento amplio de la infraestructura tecnología Sala de Computo	14/04/2016	Papelería, bolígrafos y agenda
Entrevista con el encargado de la Sala	14/04/2016	Papelería, bolígrafos y agenda
Revisión de las Instalaciones físicas	14/04/2016	Papelería, bolígrafos y agenda
Identificación de los activos Informáticos	14/04/2016	Papelería, bolígrafos y agenda
Verificación de horarios de accesos	18/04/2016	Papelería, bolígrafos y agenda
Revisión del Manual de Funciones de la Sala	18/04/2016	Papelería, bolígrafos y agenda
Niveles de seguridad para el acceso	18/04/2016	Papelería, bolígrafos y agenda
Identificación y Evaluación de Riesgos teniendo en cuenta la metodología Magerit	20/04/2016	Portátil, bolígrafos y agenda
Observación del portal institucional y verificar si la información está actualizada con la información contenida en el PEI	22/04/2016	Papelería, bolígrafos y agenda
Conocimiento del Sistema de Información SI3, procesos y funciones y verificación de usuarios que acceden al sistema	02/05/2016	Papelería, bolígrafos y agenda
Reporte de Hallazgos	12/05/2016	Papelería, bolígrafos, portátil y agenda
Informe Final	13/05/2016	Papelería, bolígrafos, portátil y agenda
Fuente: El Autor		

Teniendo en cuenta que la auditoria se realizará con el estándar COBIT, los siguientes son los dominios, procesos y objetivos que se aplicaran en la auditoria.

Dominio: PLANEAR Y ORGANIZAR (PO)

PO4 Definir procesos, organización y relaciones de TI: Verificar la prestación del servicio, definir roles, funciones y responsabilidades en TI de la institución, establecer las prioridades de los recursos de TI.

PO4.6 Establecimiento de Roles y Responsabilidades

Dominio: ADQUIRIR E IMPLEMENTAR (AI)

AI3 Adquirir y Mantener Arquitectura de TI: mantener y proteger la infraestructuctura tecnológica, mediante de planes que permita la disponibilidad de los recursos.

AI3.2 Protección y Disponibilidad del Recurso de Infraestructura
AI3.3 Mantenimiento de la Infraestructura

Dominio: ENTREGAR Y DAR SOPORTE (DS)

DS5 Garantizar la seguridad de sistemas: administrar la seguridad para proteger los activos de la institución, establecimiento de controles físicos y lógicos que permitan mejorar el buen uso de los recursos

DS5.2 Plan de Seguridad de TI
DS5.9 Prevención, Detección y Corrección de Software Malicioso

DS12 Administración del Ambiente Físico: establecer controles que proporcione un ambiente seguro y protección contra desastres naturales y fallas humanas que puedan afectar el buen funcionamiento de las instalaciones.

DS12.2 Medidas de Seguridad Física
DS12.4 Protección Contra Factores Ambientales

8.3 EJECUCIÓN

El proceso de auditoria se ejecuta siguiendo teniendo en cuenta la metodología de listas de chequeo en la institución Educativa Escuela Normal Superior de Quibdó:

Aplica (SI-NO): Indica si la implementación del control tiene aplicabilidad a nivel de la función de la organización.
N/A: Si no aplica el control se deberá indicar, y realizar la respectiva observación y así lo amerita**.**
Observaciones: Se realizarán anotaciones relacionados con el control, y otras que considere pertinentes mencionar.

8.3.1 Listas de Chequeo para la Auditoria

Cuadro 5: Lista de Chequeo 1

ESCUELA NORMAL SUPERIOR DE QUIBDÓ			
Dominio	**Planear y Organizar**		
Proceso	**PO4 Definir procesos, organización y relaciones de TI**		
Objetivo de Control	PO4.6 Establecimiento de Roles y Responsabilidades: Es necesario establecer un manual de funciones donde se especifiquen los roles y responsabilidades del personal de TI dentro de la institución.		
Cuestionario			
Pregunta	SI	**NO**	**N/A - OBSERVACIONES**
¿Cuenta la institución con manual de funciones?			
¿Se establecen los roles y responsabilidades de TI?			
¿Conoce la comunidad educativas las Funciones en TI?			
¿Hay separación de deberes dentro de la institución?			
Fuente: El Autor			

Aplicando la lista de cheque se pudo verificar que:

- La Institución educativa no cuenta con un manual de funciones para la utilización de los recursos informáticos de la sala de sistema.

- No están establecidos claramente los roles y responsabilidades dentro de los docentes quienes tiene el manejo de la sala, solo se dedican a dictar las clases a los estudiantes, pero no hay un documento que soporte y establezca las funciones dentro de la misma.

- No existe separación de deberes dentro de la misma no hay control de los recursos.

Cuadro 6: Lista de Chequeo 2

ESCUELA NORMAL SUPERIOR DE QUIBDO			
Dominio	**Adquirir e Implementar**		
Proceso	**AI3 Adquirir y Mantener Arquitectura de TI:** adquirir y proteger la infraestructuctura tecnológica, mediante de planes que permita la disponibilidad de los recursos.		
Objetivo de Control	AI3.2 Protección y Disponibilidad del Recurso de Infraestructura: establecer controles de protección para asegurar la disponibilidad de los recursos dentro de la IE		
Cuestionario			
Pregunta	SI	**NO**	**N/A - OBSERVACIONES**
¿Existe un inventario donde se identifique los activos de la IE?			
¿Se clasifica la información teniendo en cuenta las responsabilidades?			
¿Hay procedimientos para el manejo de activos?			
¿Hay procedimientos formales para disponer los medios cuando ya no se requieran?			
¿Se protegen los medios físicos que contiene información?			
Fuente: El Autor			

Aplicando la lista de chequeo número 2, se pudo verificar que:

- La institución desconoce que hay otros elementos que hacen parte de los activos informáticos, para ellos solo son los computadores, por lo cual no tiene un inventario real de sus activos.

- No hay clasificación de la información por las responsabilidades del personal dentro de la sala, pero al referirse al sistema de información si hay clasificación de la información que cada usuario puede manejar.

- No existen procedimientos para el manejo de los activos, ni para disponer de los medios cuando no se requieran, no hay protección de los medios físicos que contiene información porque en ocasiones de pierde información importante para la institución.

Cuadro 7. Lista de Chequeo 3

ESCUELA NORMAL SUPERIOR DE QUIBDÓ			
Dominio	**Adquirir e Implementar**		
Proceso	**AI3 Adquirir y Mantener Arquitectura de TI:** adquirir y proteger la infraestructuctura tecnológica, mediante de planes que permita la disponibilidad de los recursos.		
Objetivo de Control	AI3.3 Mantenimiento del Hardware y Software: establecer los procedimientos para la el mantenimiento del Hardware y software existente en la sala de informática de la IE		
Cuestionario			
Pregunta	SI	**NO**	**N/A - OBSERVACIONES**
¿Se realiza mantenimiento periódico a los computadores de la sala de sistema?			
¿Existe un cronograma de mantenimiento a los equipos de cómputos?			

¿Realiza el mantenimiento alguien de la IE?			
Fuente: El Autor			

Aplicando la lista de cheque 3 se verificó que:

- Dentro de la sala no se realiza mantenimiento periódico, la persona que está encargado a veces lo realiza con los practicantes del SENA.

- No existe un cronograma para el mantenimiento periódico de las salas cuando hay muy esporádicamente se realiza el mantenimiento, lo realizan estudiantes del SENA con el docente encargado de la sala.

Cuadro 8. Lista de Chequeo 4

ESCUELA NORMAL SUPERIOR DE QUIBDÓ			
Dominio	**Entregar y Dar Soporte**		
Proceso	**DS5 Garantizar la seguridad de sistemas:** administrar la seguridad para proteger los activos de la institución, establecimiento de controles físicos y lógicos que permitan mejorar el buen uso de los recursos.		
Objetivo de Control	DS5.9 Prevención, Detección y Corrección de Software Malicioso. Establecer las medidas preventivas y correctivas para proteger el hardware y el software de la institución contra malware (virus, gusanos, spyware, correo basura).		
Cuestionario			
Pregunta	SI	**NO**	**N/A - OBSERVACIONES**
¿Tiene plan para protección de registros?			
¿Se establece condiciones y términos de servicios?			
¿Hace control para evitar la propagación de código Malicioso?			
¿Utiliza medida de protección de los contra código malicioso?			
¿Existe Manual de procedimientos documental?			

¿Existe manual de políticas de respaldo de la información?			
¿Cuenta la institución con antivirus legalizado y dentralizado?			
Fuente: El Autor			

Con la lista de chequeo 4, se observó que:

- No cuentan con un plan de protección de los registros, solo los ingresan al sistema de información y se sacan los reportes, pero no tiene el control total de los datos ya que los tiene el proveedor del sistema de información.

- No hay establecimiento de términos y condiciones para el manejo de la información y los recursos.

- No existe control para evitar la propagación de código malicioso porque es lo que frecuentemente ocurre dentro de la sala y es la mayor causa del deterioro de los computadores por la presencia de virus. Por lo cual no hay medida de protección para evitar su propagación.

- No existe manual de procedimientos ni manual de política de respaldo.

- No hay antivirus legalizado.

Cuadro 9. Lista de Chequeo 5

ESCUELA NORMAL SUPERIOR DE QUIBDÓ	
Dominio	**Entregar y Dar Soporte**
Proceso	**DS5 Garantizar la seguridad de sistemas:** administrar la seguridad para proteger los activos de la institución, establecimiento de controles físicos y lógicos que permitan mejorar el buen uso de los recursos.
Objetivo de Control	DS5.2 Plan de Seguridad de TI: Establecimiento del plan de Seguridad informática que garantice la disponibilidad, confidencialidad e integridad de la

	información y de la infraestructura tecnológica		
Cuestionario			
Pregunta	SI	**NO**	**N/A - OBSERVACIONES**
¿Cuenta la IE con política de seguridad de la información, que incluya aspectos físicos como lógicos?			
¿Se da a conocer la política de seguridad de la Información a los miembros de la IE?			
¿Se revisa las políticas para la seguridad de la información?			
Fuente: El Autor			

Se aplicó la lista de chequeo 5 y se observó:

- No existe una política de seguridad e la información que incluya aspectos físicos y lógicos, por lo cual no se tiene en cuenta los puntos de dar a conocer y revisar la política, debido a la ausencia de la misma.

Cuadro 10. Lista de Chequeo 6

ESCUELA NORMAL SUPERIOR DE QUIBDO			
Dominio	**Entregar y Dar Soporte**		
Proceso	**DS12 Administración del Ambiente Físico:** establecer controles que proporcione un ambiente seguro y protección contra desastres naturales y fallas humanas que puedan afectar el buen funcionamiento de las instalaciones.		
Objetivo de Control	DS12.2 Medidas de Seguridad Física: Establecimiento de controles de seguridad física.		
Cuestionario			
Pregunta	SI	**NO**	**N/A - OBSERVACIONES**
¿Se ha establecido controles de seguridad física?			
¿Tiene plan ante la falla del sistema de seguridad?			
¿Se registran las personas que ingresan a las instalaciones de la Institución?			
¿Se encuentra definido el perímetro de			

Seguridad Física?			
¿Existe Política de control de Acceso a las Instalaciones?			
¿Hay mecanismos de protección frente a amenazas externas?			
¿Se trabaja en áreas seguras?			
¿Hay política de equipos desatendidos?			
¿Se controla el retiro de activos en la IE?			
Fuente: El Autor			

En la lista de chequeo 6 se observó que:

- No hay controles de seguridad física que garantice la seguridad del área.

- No hay plan ante la falla del sistema de seguridad.

- No se registran las personas que ingresan al aula ni a la institución.

- No está definido el perímetro de seguridad de la institución ni de la sala de informática.

- No existe política de control de control de acceso alas instalaciones de la institución.

- En cuanto a la protección frente amenazas externas, solo esta el vigilante de la puerta principal de la institución el cual no tiene control sobre otras áreas que pueden acceder personas inescrupulosas por lo cual no se considera un área segura porque es blanco de acceso por la ausencia de un ben sistema de vigilancia.

- No hay políticas y procedimientos para los equipos desatendidos, no se controla claramente el retiro de activos de la institución, pues quien da el permiso es el rector de la IE.

Cuadro 11. Lista de Chequeo 7

ESCUELA NORMAL SUPERIOR DE QUIBDÓ			
Dominio	**Entregar y Dar Soporte**		
Proceso	**DS12 Administración del Ambiente Físico:** establecer controles que proporcione un ambiente seguro y protección contra desastres naturales y fallas humanas que puedan afectar el buen funcionamiento de las instalaciones.		
Objetivo de Control	DS12.4 Protección Contra Factores Ambientales: Establecer políticas de control de acceso al aula de informática para proteger contra factores ambientales.		
Cuestionario			
Pregunta	SI	**NO**	**N/A - OBSERVACIONES**
¿Existe detector de Humo?			
¿Hay control de Seguridad de acceso a lugares restringidos?			
¿Se ha encontrado alguna falla en el control?			
¿Se trabaja en áreas seguras?			
¿Existe protección del cableado de energía eléctrica y de telecomunicaciones?			
¿Cuenta la sala con espacio amplio para facilitar la movilización?			
Existe Señalización de Zonas de Evacuación?			
¿Existen extintores?			
¿Existe Sistema de ventilación?			
¿Cuenta la institución con avisos de prohibición de fumar, comer, e ingresar			

líquidos a la sala?			
¿Se la hace seguimiento a las prohibiciones?			
¿Existe esquema de conexión eléctrica con interruptores?			
Fuente: El Autor			

Después de aplicarse la lista de chequeo 7 se observó:

- La institución no cuenta con detector de humo.
- No hay zonas marcadas con acceso restringido, todos pueden acceder los recursos de la sala.
- El área no se considera segura porque solo tiene una puerta de acceso sin mucha seguridad, las instalaciones y tablero eléctrico se encuentran dentro de la sala propensa a cualquier corto que pueda colocar en peligro a los estudiantes que acceden a ella.
- La protección del cableado eléctrico, existen canaletas de protección, pero se encuentran en mantenimiento.
- No cuenta con espacio amplio que facilite la movilización en ocasiones se observa que es muy estrecha en comparación a la cantidad de estudiantes de un curso.
- Si hay un extintor, el cual se desconoce cómo se utiliza.
- No hay señalización de la zona de evacuación.
- Cuenta con un aire acondicionado el cual no es suficiente porque hace mucho calor y el sol penetra por las ventanas.
- No cuenta la institución con avisos de prohibición de fumar, comer e ingresar líquidos a la sala, esto lo hacen los docentes, pero no hay procedimiento formal para estas restricciones.

- Cuenta con un esquema de conexión eléctrica con interruptores, pero está dentro del aula.

8.3.1 Visita a las Instalaciones de la Institución

Se realizaron las visitas para conocer las instalaciones del aula informática, en dicha visita se realizó la entrevista con el encargado de la Sala Informática, se identificaron los siguientes activos que se detallas en el siguiente cuadro:

Cuadro 12. Activos Informáticos

Tipo de activo	Descripción
Hardware	Portátiles de computadores para educar y computadores de escritorio
Datos/ Información	Información de Estudiantes, docentes y directivos
	Calificaciones
Software	Sistema de notas SI3
	Sistema Operativo Windows
	Portal Institucional
Redes de Comunicaciones	Switche
	Red cableada e inalámbrica
Equipamiento Auxiliar	Extintor
	Video Beam
Seguridad Física	Cableado Estructurado
	Instalaciones
	Instalaciones eléctricas
Talento Humano	Docentes, estudiantes, coordinador, auxiliares
Fuente: El Autor	

8.3.3 Identificación de Amenazas

El proceso de identificación de amenazas a los activos mediante la metodología Magerit, se relacionan a continuación:

Cuadro 13. Identificación de Amenazas

Recursos Afectados	**Amenazas**	**Dimensiones de seguridad**
Hardware	[N.1] Fuego: incendio	Disponibilidad [D]
	[N.*] Desastres naturales	Disponibilidad [D]
	[I.5] Avería de origen físico o lógico:	Disponibilidad [D]
	[I.6] Corte del suministro eléctrico	Disponibilidad
	[I.7] Condiciones inadecuadas de temperatura o humedad: Exceso de calor	Disponibilidad
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
	[E.25] Robo	D] disponibilidad [C] confidencialidad
	[A.26] Ataque destructivo	[D] disponibilidad
Software	[I.5] Avería de origen físico o lógico	Disponibilidad [D]
	[E.1] Errores de los usuarios	[I] integridad [C] confidencialidad [D] disponibilidad
	[E.8] Difusión de software dañino: propagación de virus	[D] disponibilidad [I] integridad [C] confidencialidad
	[E.20] Vulnerabilidades de los programas (software)	[I] integridad [D] disponibilidad [C] confidencialidad
	[E.21] Errores de mantenimiento / actualización de programas (software)	[I] integridad [D] disponibilidad
Datos	[E.1] Errores de los usuarios	[I] integridad [C] confidencialidad [D] disponibilidad
Equipamiento Auxiliar	[N.1] Fuego: incendio	Disponibilidad [D]
	[N.*] Desastres naturales	Disponibilidad [D]
	[I.5] Avería de origen físico o lógico:	Disponibilidad [D]

	[I.6] Corte del suministro eléctrico	Disponibilidad [D]
	[I.7] Condiciones inadecuadas de temperatura o humedad: Exceso de calor	Disponibilidad
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
	[E.25] Robo	D] disponibilidad [C] confidencialidad
	[A.26] Ataque destructivo	[D] disponibilidad
Instalaciones	[A.26] Ataque destructivo	[D] disponibilidad
	[N.1] Fuego: incendio	Disponibilidad [D]
	[N.*] Desastres naturales	Disponibilidad [D]
Personal	[E.7] Deficiencia en las organizaciones	Disponibilidad
	[A.28] Indisponibilidad del personal	[D] disponibilidad
Fuente: Magerit Libro I		

8.3.4 Estimación del Riesgo

Se tendrá en cuenta la frecuencia de ocurrencia del riesgo, el impacto basado en los siguientes criterios

Frecuencia:

Muy frecuente MF
Frecuente F
Normal FN
Poco frecuente PF

Impacto:

MA: Muy Alto (4)
A: Alto (3)
M: Medio (2)
B: Bajo (1)
MB: Muy Bajo

Cuadro 14: Valoración del Riesgo

Recursos Afectados	Amenazas	Impacto			F	Riesgo
		D	I	C		
Hardware	[N.1] Fuego: incendio	MA	B	B	PF	B
	[N.*] Desastres naturales	MA	MB	MB	PF	B
	[I.5] Avería de origen físico o lógico:	MA	B	B	F	A
	[I.6] Corte del suministro eléctrico	A	B	B	F	A
	[I.7] Condiciones inadecuadas de temperatura o humedad: Exceso de calor	A	B	B	F	M
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	MA	M	M	NF	A
	[E.25] Robo	A	B	A	PF	M
	[A.26] Ataque destructivo	A	B	B	PF	B
Software	[I.5] Avería de origen físico o lógico	MA	B	B	F	A
	[E.1] Errores de los usuarios	A	A	A	FN	A
	[E.8] Difusión de software dañino: propagación de virus	MA	MA	MA	MF	MA
	[E.20] Vulnerabilidades de los programas	A	A	A	F	A

	(software)					
	[E.21] Errores de mantenimiento / actualización de programas (software)	A	A	B	MF	A
Datos	[E.1] Errores de los usuarios	A	A	A	FN	A
Equipamiento Auxiliar	[N.1] Fuego: incendio	MA	B	B	PF	B
	[N.*] Desastres naturales	MA	MB	MB	PF	B
	[I.5] Avería de origen físico o lógico:	MA	B	B	F	A
	[I.6] Corte del suministro eléctrico	A	B	B	F	A
	[I.7] Condiciones inadecuadas de temperatura o humedad: Exceso de calor	A	B	B	F	M
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	MA	M	M	NF	A
	[E.25] Robo	A	B	A	PF	M
	[A.26] Ataque destructivo	A	B	B	PF	B
Instalaciones	[A.26] Ataque destructivo	A	B	B	PF	B
	[N.1] Fuego: incendio	MA	B	B	PF	B
	[N.*] Desastres naturales	MA	MB	MB	PF	B
Personal	[E.7] Deficiencia en las organizaciones	MA	B	B	FN	M
	[A.28] Indisponibilidad	A	MB	MB	FN	M

	del personal					
Fuente: El Autor						

8.4. HALLAZGOS

Una vez realizada la fase de ejecución donde se identificación, se clasificaron los riesgos se da informe sobre los hallazgos encontrados en cada objetivo de control de COBIT, a continuación, se describen:

Dominio: Planear y Organizar
Proceso: PO4 Definir procesos, organización y relaciones de TI
Objetivo de Control: Establecimiento de Roles y Responsabilidades
Nivel de Madurez: 0
Riesgos Asociados: Medio
Resultados: La Institución no cuenta con una estructura organizacional de TI, ni cuenta con un manual de funciones de la sala, donde se especifique los roles y responsabilidad de utilización de recursos, referente al sistema SI3, están definidas las responsabilidad y privilegios de acceso, pero no hay un manual que soporte.
Recomendaciones: Establecer un manual para el establecimiento de roles y responsabilidades en la utilización de los activos informáticos, que garantice el buen uso de los mismo.

Dominio: Adquirir e Implementar
Proceso: AI3 Adquirir y Mantener Arquitectura de TI
Objetivo de Control: Protección y Disponibilidad del Recurso de Infraestructura
Nivel de Madurez: 1
Riesgos: Alto
Resultados: La Institución no cuenta con un inventario de activos, hay procedimientos formales que implique el manejo de activos, no existe una política para el tratamiento de activos e información, donde le permita establecer mecanismos para realizar el uso adecuado de los mismos.
Recomendaciones: La institución debe realizar el proceso de identificación de los activos informáticos, establecer políticas para el uso de ellos.

Dominio: Adquirir e Implementar
Proceso: AI3 Adquirir y Mantener Arquitectura de TI
Objetivo de Control: Mantenimiento del Hardware y Software
Nivel de Madurez: 1
Riesgos: Alto

Resultados: La Institución no cuenta con un cronograma periódico de mantenimiento de equipos preventivo y correctivo, en ocasiones son realizados por estudiantes del SENA.
Recomendaciones: La institución debe realizar un cronograma de mantenimiento periódico a los equipos, de la forma que le ayude a prevenir daños y desconfiguración de los computadores.

Dominio: Entregar y dar Soporte
Proceso: DS5 Garantizar la seguridad de sistemas
Objetivo de Control: Prevención, Detección y Corrección de Software Malicioso
Nivel de Madurez: 1
Riesgos Asociados: Medio
Resultados: La Institución no cuenta con: Un plan de protección de registros, no se hace control para evitar la propagación de código malicioso, no hay manual de procedimientos documental, no cuenta con antivirus adecuado, cuenta con un antivirus que no realiza buena protección a los equipos, en ocasiones se pierde información por la existencia de código malicioso, no es centralizado.
Recomendaciones: La institución debe establecer un plan de protección de los registros, establecer procedimientos de detención, prevención y corrección de software malicioso (Virus, troyanos, spyware, etc.).

Dominio: Entregar y dar Soporte
Proceso: DS5 Garantizar la seguridad de sistemas
Objetivo de Control: Plan de Seguridad de TI
Nivel de Madurez: 0
Riesgos Asociados: Muy Alto
Resultados: La Institución no cuenta con una política de seguridad de TI, ni con un plan que garantice la seguridad de los activos informáticos.
Recomendaciones: La institución debe establecer un plan de seguridad de TI, debido a que muchos problemas de seguridad que poseen se puede resolver con el establecimiento de una política clara en materia de seguridad de TI, este plan les permitirá, identificar prevenir y corregir las fallas, establecimiento de controles y roles dentro de los mismo.

Dominio: Entregar y dar Soporte
Proceso: DS12 Administración del Ambiente Físico
Objetivo de Control: Medidas de Seguridad Física
Nivel de Madurez: 0
Riesgos Asociados: Alto
Resultados: La Institución no cuenta con controles de seguridad física, no hay un plan de seguridad física, no hay registros de las personas que ingresan al aula,

solo el horario que identifica los estudiantes que están en clase de informática, no hay definido perímetro de seguridad física definido, solo cuanta con un extintor que se desconoce el uso, no hay mecanismos de protección contra amenazas externas, no hay política de retiro de activos.
Recomendaciones: La institución debe establecer un plan de seguridad de física que contenga: controles, plan de ante la falla del sistema de seguridad, establecer política control de acceso a las instalaciones, definir el perímetro de seguridad física, establecer mecanismos de protección contra amenazas externas.

Dominio: Entregar y dar Soporte
Proceso: DS12 Administración del Ambiente Físico
Objetivo de Control: Protección Contra Factores Ambientales
Nivel de Madurez: 1
Riesgos Asociados: Medio
Resultados: La Institución no con una política de control de acceso al aula de informática, no existe detector de humo, no hay control de seguridad de acceso, no hay zonas marcadas como restringida, el área de no se considera segura, por el momento la sala no cuenta con protección de redes eléctricas y de red, porque se está organizando y estructurando nuevamente, la sala es pequeña lo cual no facilita la movilización y mucho más si las personas son discapacitados físicos, a pesar de tener un aire acondicionado, no es suficiente la ventilación, no están marcada la zona de evacuación, no tiene avisos de prohibición de fumar, comer, e ingresar líquidos a la sala, hay un extintor pero no se tiene muchas claridad sobre el uso.
Recomendaciones: Establecer un plan de protección contra factores ambientales, elaborar un mapa de riesgos físicos que pueda contrarrestar los riesgos existentes en la actualidad.

8.5 INFORME FINAL

A continuación, se presenta el informe con los resultados definitivos de la auditoria, las observaciones de cada uno de los Objetivos de COBIT aplicados y sus respectivas recomendaciones para tener en cuenta las directivas de la Institución educativa.

Fecha: 30/05/2016

Nombre de la Entidad: Institución Educativa Escuela Normar Superior de Quibdó
AUDITORIA INFORMÁTICA A LA INFRAESTRUCTURA TECNOLÓGICA Y SISTEMAS DE INFORMACIÓN BAJO EL ESTÁNDAR COBIT.

Objetivo

Evaluar la seguridad informática de la infraestructura tecnológica y sistemas de información en la Institución Educativa Escuela Normal Superior de Quibdó.

Alcance

Se evaluará la gestión administrativa de la sala de cómputo, cumplimiento de las funciones y prestación de servicios, infraestructura física, seguridad física, ubicación, infraestructura eléctrica, redes, Gestión y actualización de la información, Usuarios que acceden al sistema, utilización de la información.

Objetivos de Control Cobit Aplicados en la Auditoria

Objetivo de Control: Establecimiento de Roles y Responsabilidades
Observación: En la entrevista con el coordinador de la sala de informática y personal administrativo de la Institución no se evidencio una estructura organizacional de TI, ni con un manual de funciones de la sala, donde se especifique los roles y responsabilidad de utilización de recursos, referente al sistema SI3, están definidas las responsabilidad y privilegios de acceso, pero no hay un manual que soporte.
Recomendaciones: Establecer un manual para el establecimiento de roles y responsabilidades en la utilización de los activos informáticos, que garantice el buen uso de los mismo.

Objetivo de Control: Protección y Disponibilidad del Recurso de Infraestructura
Observación: En la entrevista con el coordinador de la sala de informática, el rector de la institución y coordinador académico, se evidenció que la Institución no cuenta con un inventario de activo, no hay procedimientos formales que implique el manejo de activos, no existe una política para el tratamiento de activos e información, donde le permita establecer mecanismos para realizar el uso adecuado de los mismos.
Recomendaciones: La institución debe realizar el proceso de identificación de los activos informáticos, establecer políticas para el uso de ellos.

Objetivo de Control: Mantenimiento del Hardware y Software
Observación: En la entrevista con el coordinador de la sala de informática, se evidenció que la Institución no cuenta con un cronograma periódico de mantenimiento de equipos preventivo y correctivo, en ocasiones son realizados por estudiantes del SENA.
Recomendaciones: La institución debe realizar un cronograma de mantenimiento periódico a los equipos, de la forma que le ayude a prevenir daños y desconfiguración de los computadores.

Objetivo de Control: Prevención, Detección y Corrección de Software Malicioso
Observación: En la entrevista con el coordinador de la sala de informática, se evidenció que la Institución no cuenta con: Un plan de protección de registros, no se hace control para evitar la propagación de código malicioso, no hay manual de procedimientos documental, no cuanta con antivirus potente, cuenta con un antivirus que no realiza buena protección a los equipos, en ocasiones se pierde información por la existencia de código malicioso.
Recomendaciones: La institución debe establecer un plan de protección de los registros, establecer procedimientos de detención, prevención y corrección de software malicioso (Virus, troyanos, spyware, etc.).

Objetivo de Control: Plan de Seguridad de TI
Observación: En la entrevista con el coordinador de la sala de informática y el rector, se evidenció que la Institución no cuenta con una política de seguridad de TI, ni con un plan que garantice la seguridad de los activos informáticos.
Recomendaciones: La institución debe establecer un plan de seguridad de TI, debido a que muchos problemas de seguridad que poseen se puede resolver con el establecimiento de una política clara en materia de seguridad de TI, este plan les permitirá, identificar prevenir y corregir las fallas, establecimiento de controles y roles dentro de los mismo.

Objetivo de Control: Medidas de Seguridad Física
Observación: En la entrevista con el coordinador de la sala de informática, se evidenció que la Institución no cuenta con controles de seguridad física, no hay un plan de seguridad física, no hay registros de las personas que ingresan al aula, solo el horario que identifica los estudiantes que están en clase de informática, no hay definido perímetro de seguridad física definido, solo cuenta con un extintor que se desconoce el uso, no hay mecanismos de protección contra amenazas externas, no hay política de retiro de activos.
Recomendaciones: La institución debe establecer un plan de seguridad de física que contenga: controles, plan de ante la falla del sistema de seguridad, establecer política control de acceso a las instalaciones, definir el perímetro de seguridad física, establecer mecanismos de protección contra amenazas externas.

Objetivo de Control: Protección Contra Factores Ambientales
Observación: En la entrevista con el coordinador de la sala de informática, personal administrativos, docentes y estudiantes, se evidenció que la Institución no con una política de control de acceso al aula de informática, no existe detector de humo, no hay control de seguridad de acceso, no hay zonas marcadas como restringida, el área de no se considera segura, por el momento la sala no cuenta con protección de redes eléctricas y de red, porque se está organizando y estructurando nuevamente, la sala es pequeña lo cual no facilita la movilización y mucho más si las personas son discapacitados físicos, a pesar de tener un aire acondicionado, no es suficiente la ventilación, no están marcada la zona de evacuación, no tiene avisos de prohibición de fumar, comer, ingresar líquidos a la sala, hay un extintor pero no se tiene muchas claridad sobre el uso.
Recomendaciones: Establecer un plan de protección contra factores ambientales, elaborar un mapa de riesgos físicos que pueda contrarrestar los riesgos existentes en la actualidad.

Propuestas acciones preventivas y de mejora:

La Institución debe:

- Asignar recursos económicos para la consecución de herramientas de seguridad que permitan proteger los activos más importantes de la institución.
- Sensibilizar a la comunidad educativa acerca de la aplicación y cumplimiento de lo establecido en los protocolos de confidencialidad de la información, tratamiento de datos y manuales para uso adecuado de la infraestructura tecnológica.
- Analizar la administración de riesgos informáticos, amenazas y vulnerabilidades detectadas y tomar decisiones frente a los hallazgos encontrados en el desarrollo del proyecto.

- Atender las recomendaciones realizadas por cada uno de los hallazgos.
- Proteger mediante acciones y políticas ante los posibles riesgos que pueden poner en peligro la prolongación de los niveles de competitividad, rentabilidad y conformidad legal, necesarios para alcanzar los objetivos de la institución, lo que permite reducir los riesgos a los que se exponen la seguridad de la organización.
- Elaborar un plan de Auditoria para establecer mecanismos que garanticen la seguridad informática.

9. CONCLUSIÓN

En esta investigación se da cumplimiento a los objetivos de la misma, se identificaron los elementos a auditar en la Institución Educativa, el cual contó el apoyo del rector de la Institución, inicialmente se tenía previsto la evaluación del Sistema de Información, pero no se pudo realizar por los siguientes aspectos:

- El operador del aplicativo de notas SI3 según lo contratado con la Institución, son los encargados del soporte técnico y garantizarle la seguridad, es un aplicativo en línea y cuenta con servidores de bases de datos y de aplicaciones, los cuales no son activos de la institución.
- El operador se encuentra en proceso de actualización de mejora del aplicativo.

Se elaboró el plan de auditoria para su posterior ejecución, se realizó la identificación y valoración de riesgos teniendo en cuenta la metodología Magerit, mediante las listas de chequeo se ejecutó verificando el cumplimiento de los objetivos de control de Cobit aplicables en esta auditoría, se realizó un informe con los hallazgos y recomendaciones para las directivas de la Institución.

Los resultados obtenidos en el proceso de auditoría a la infraestructura tecnológica y sistemas de información en la Escuela Normal Superior de Quibdó le permitirá a las directivas de la institución Educativa diseñar e implementar un plan de Seguridad de la Información que involucre a toda la comunidad educativa para que se tome conciencia de la importancia de la seguridad de la información, lo cual permita reducir el nivel de riesgo, igualmente se debe implementar un plan de protección de las instalaciones, realizar un mapa de riesgos físico, realizar señalizaciones y otros aspectos que conlleven al buen funcionamiento y uso de los recursos.

Teniendo en cuenta lo anterior se concluye que el proyecto es de gran ayuda a para la institución porque les permite tener una evaluación clara del funcionamiento de sus activos informáticos y lo que se debe hacer para reducir los riesgos a los que se encuentran expuestos y así mejorar la seguridad informática de la institución.

.

10. DIVULGACIÓN

La divulgación se hará mediante un informe final de la auditoría presentado a las directivas de la institución, contiene los hallazgos, acciones correctivas y controles propuestos para establecer un plan de mejoramiento de la seguridad informática y de la información.

BIBLIOGRAFÍA

ARBOLEDA, Nicolas Ibarguen. 2012**.** Reseña Historica de lLa E.N.S.Q. [En línea]. Jun. 2012 [Citado el: 30 de 08 de 2014]. Disponible en internet: < URL: http://escuelanormalquibdo.blogspot.com.co/>

BAHAMONTES, Ángel. Auditoría de Seguridad Informática . [En línea]. Asociación Nacional de Tasadores y Peritos Judiciales Informáticos, 15 de agosto de 2013. [Citado el: 22 de septiembre de 2015.]. Disponible en Disponible en internet: < URL: http://www.antpji.com/antpji2013/index.php/articulos2/111-auditoria-de-seguridad-informatica >

ISACA. Cobit 4.1. [En Línea]. 2007. [Citado el 1 de diciembre de 2015]. Disponible Disponible en internet: < URL: http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf>

ISACA. Cobit 5 Introduccion. [En Línea]. 2007. [Citado el 1 de diciembre de 2017]. Disponible Disponible en internet: < URL: http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx>

ELISSONDO, Luis**.** Auditoría y Seguridad de Sistemas de Información. [En línea] [Citado el: 20 de septiembre de 2015.] Disponible Disponible en internet: < URL: http://econ.unicen.edu.ar/monitorit/index.php?option=com_docman&task=doc_download&gid=404&Itemid=19>

ESCUELA NORMAL SUPERIOR DE QUIBDÓ. Portal Institucional. [En línea] [Citado el: 30 de 08 de 2015.]. Disponible e Disponible en internet: < URL: http://ienormalquibdo.edu.co/portal/>

GOBIERNO DE ESPAÑA. MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I [En línea] [Citado el: 15 de 09 de 2015.]. Disponible Disponible en internet: < URL: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VsZ4EbbhDIU>

GIRALDO, Carlos Andres y MARTINEZ, Jhon Edinson. Auditoria de Seguridad Informatica. [En línea] [Citado el: 15 de Septiembre de 2015.] Disponible en internet: < URL: http://artemisa.unicauca.edu.co/~ecaldon/docs/audit/ponencia_PASSWORD_siti2004.pdf. >

Auditoría Informática. [En línea] [Citado el: 03 de 10 de 2015.] Disponible en internet: < URL: http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml.>

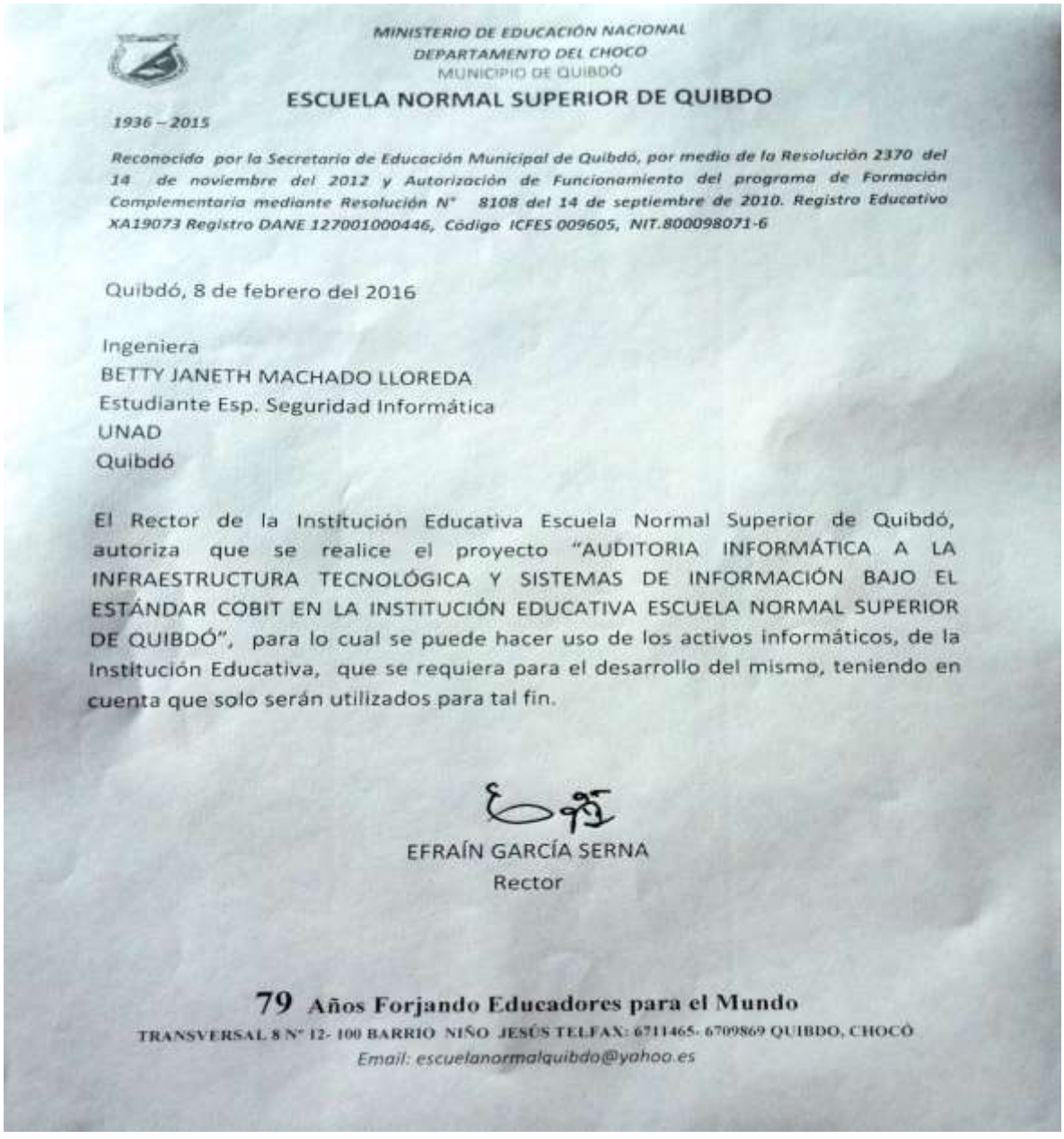
RUIZ, Alberto Jimez**.** myEchelon: Un sistema de Auditoría de Seguridad Informatica Avanzado bajo GNU/Linux. [En línea] Universidad de Almeria. [Citado el: 20 de septiembre de 2015.]. Disponible en internet: < URL: http://www.adminso.es/images/9/9c/Alberto_PFC.pdf.>

SÁNCHEZ, Esmeralda Guindel. Calidad y Seguridad de la Información y Auditoria Informática. [En línea] UNIVERSIDAD CARLOS III DE MADRID , 23 de noviembre de 2009. [Citado el: 20 de septiembre de 2015.]. Disponible en: http://e-archivo.uc3m.es/bitstream/handle/10016/8510/proyectoEsmeralda.pdf?sequence=1.

SOLARTE, Francisco Nicolas. 2011. Auditoría Informática y de Sistemas. [En línea] 30 de noviembre de 2011. [Citado el: 20 de septiembre de 2015.]. Disponible en internet: < URL: http://auditordesistemas.blogspot.com.co/2011/11/metodologia-para-realizar-auditoria.html.>

ANEXOS

ANEXO A. Carta de Autorización para realizar el proyecto en la IE



MINISTERIO DE EDUCACIÓN NACIONAL
DEPARTAMENTO DEL CHOCO
MUNICIPIO DE QUIBDÓ

ESCUELA NORMAL SUPERIOR DE QUIBDO

1936 – 2015

Reconocido por la Secretaria de Educación Municipal de Quibdó, por medio de la Resolución 2370 del 14 de noviembre del 2012 y Autorización de Funcionamiento del programa de Formación Complementaria mediante Resolución N° 8108 del 14 de septiembre de 2010. Registro Educativo XA19073 Registro DANE 127001000446, Código ICFES 009605, NIT.800098071-6

Quibdó, 8 de febrero del 2016

Ingeniera
BETTY JANETH MACHADO LLOREDA
Estudiante Esp. Seguridad Informática
UNAD
Quibdó

El Rector de la Institución Educativa Escuela Normal Superior de Quibdó, autoriza que se realice el proyecto "AUDITORIA INFORMÁTICA A LA INFRAESTRUCTURA TECNOLÓGICA Y SISTEMAS DE INFORMACIÓN BAJO EL ESTÁNDAR COBIT EN LA INSTITUCIÓN EDUCATIVA ESCUELA NORMAL SUPERIOR DE QUIBDÓ", para lo cual se puede hacer uso de los activos informáticos, de la Institución Educativa, que se requiera para el desarrollo del mismo, teniendo en cuenta que solo serán utilizados para tal fin.

EFRAÍN GARCÍA SERNA
Rector

79 Años Forjando Educadores para el Mundo
TRANSVERSAL 8 N° 12- 100 BARRIO NIÑO JESÚS TELFAX: 6711465- 6709869 QUIBDO, CHOCÓ
Email: escuelanormalquibdo@yahoo.es

Fuente: Rector IE Escuela Normal Superior de Quibdó

ANEXO B. Presupuesto

Recursos Auxiliares			
Descripción	**Cantidad**	**Valor Unidad**	**Valor total**
Resma de Papel	1	$ 9.000	$ 9.000
Tóner Tinta	1	$ 90.000	$ 90.000
Fotocopias		$ 30.000	$ 30.000
Total recursos Auxiliares			**$ 129.000**
Recursos Tecnológicos			
Descripción	**Cantidad**	**Valor Unidad**	**Valor Total**
CD	3	$1.000	$ 3.000
USB	1	$ 15.000	$ 15.000
Portátil	1	$ 1.200.000	$ 1.200.000
Total recursos Tecnológicos			**1.218.000**
Imprevistos			$ 500.000
Transporte			$ 500.000
Total			**$ 2.347.000**
Fuente: El Autor			

ANEXO C: Carta de Presentación del Informe Final

Quibdó, mayo 30 de 2016

Especialista
EFRAÍN GARCÍA SERNA
Rector
Escuela Normal Superior de Quibdó
Ciudad

Ref.: Presentación de Resultados de Auditoria

Cordial Saludo

Me permito presentar el informe final de la auditoria informática a la Infraestructura Tecnológica y Sistemas de Información de la Institución Educativa que usted a bien dirige; se evaluaron los siguientes aspectos:

Sala de Informática: Seguridad Física, instalaciones, gestión Administrativa.
El funcionamiento del sistema de Información.
Actualización de la Información del Portal Institucional.

Dentro de los hallazgos encontrados en la auditoría están:
Ausencia de un manual de funciones
Debilidades en la seguridad física
Ausencia de mecanismos de prevención de Riesgos contra factores ambientales.
Ausencia de política de seguridad informática.

Anexo a esta carta se presenta el informe Final, con las respectivas recomendaciones.

Atentamente,

BETTY JANETH MACHADO LLOREDA
C.C. 26.274.426 de Quibdó
Auditor

ANEXO D: Lista de Chequeo 1

Figura 5. Lista de Chequeo 1

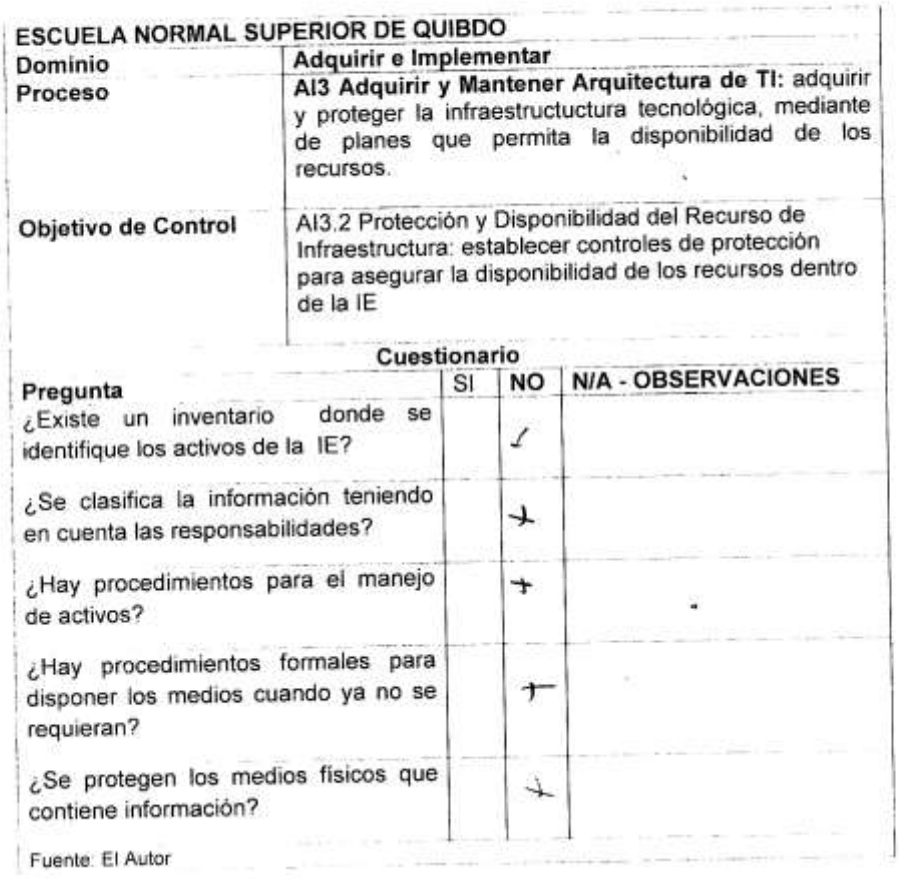
ESCUELA NORMAL SUPERIOR DE QUIBDÓ			
Dominio	**Planear y Organizar**		
Proceso	**PO4 Definir procesos, organización y relaciones de TI**		
Objetivo de Control	PO4.6 Establecimiento de Roles y Responsabilidades: Es necesario establecer un manual de funciones donde se especifiquen los roles y responsabilidades del personal de TI dentro de la institución.		
Cuestionario			
Pregunta	**SI**	**NO**	**N/A - OBSERVACIONES**
¿Cuenta la institución con manual de funciones?		X	
¿Se establecen los roles y responsabilidades de TI?		X	
¿Conoce la comunidad educativas las Funciones en TI?		X	
¿Hay separación de deberes dentro de la institución?		X	

Fuente: El Autor

Fuente: El autor

ANEXO E: Lista de Chequeo 2

Figura 6. Lista de Chequeo **2**



ESCUELA NORMAL SUPERIOR DE QUIBDO

Dominio	**Adquirir e Implementar**
Proceso	**AI3 Adquirir y Mantener Arquitectura de TI:** adquirir y proteger la infraestructuctura tecnológica, mediante de planes que permita la disponibilidad de los recursos.
Objetivo de Control	AI3.2 Protección y Disponibilidad del Recurso de Infraestructura: establecer controles de protección para asegurar la disponibilidad de los recursos dentro de la IE

Cuestionario

Pregunta	SI	NO	N/A - OBSERVACIONES
¿Existe un inventario donde se identifique los activos de la IE?		✓	
¿Se clasifica la información teniendo en cuenta las responsabilidades?		✓	
¿Hay procedimientos para el manejo de activos?		✓	
¿Hay procedimientos formales para disponer los medios cuando ya no se requieran?		✓	
¿Se protegen los medios físicos que contiene información?		✓	

Fuente: El Autor

Fuente: El Autor

ANEXO F: Lista de Chequeo 3

Figura 7. Lista de Chequeo 3

ESCUELA NORMAL SUPERIOR DE QUIBDÓ

Dominio	**Adquirir e Implementar**
Proceso	**AI3 Adquirir y Mantener Arquitectura de TI:** adquirir y proteger la infraestructuctura tecnológica, mediante de planes que permita la disponibilidad de los recursos.
Objetivo de Control	AI3.3 Mantenimiento del Hardware y Software: establecer los procedimientos para la el mantenimiento del Hardware y software existente en la sala de informática de la IE

Cuestionario

Pregunta	SI	NO	N/A - OBSERVACIONES
¿Se realiza mantenimiento periódico a los computadores de la sala de sistema?		X	
¿Existe un cronograma de mantenimiento a los equipos de cómputos?		X	
¿Realiza el mantenimiento alguien de la IE?		X	

Fuente: El Autor

Fuente: El Autor

ANEXO G: Lista de Chequeo 4

Figura 8. Lista de Chequeo 4

ESCUELA NORMAL SUPERIOR DE QUIBDÓ

Dominio	**Entregar y Dar Soporte**
Proceso	**DS5 Garantizar la seguridad de sistemas:** administrar la seguridad para proteger los activos de la institución, establecimiento de controles físicos y lógicos que permitan mejorar el buen uso de los recursos.
Objetivo de Control	DS5.9 Prevención, Detección y Corrección de Software Malicioso. Establecer las medidas preventivas y correctivas para proteger el hardware y el software de la institución contra malware (virus, gusanos, spyware, correo basura).

Cuestionario

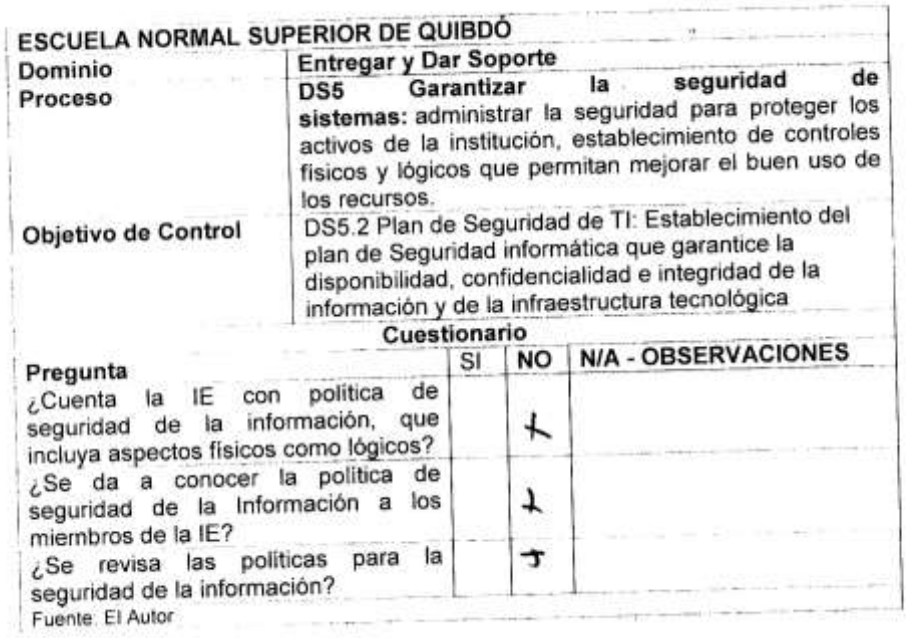
Pregunta	SI	NO	**N/A - OBSERVACIONES**
¿Tiene plan para protección de registros?		+	
¿Se establece condiciones y términos de servicios?		+	
¿Hace control para evitar la propagación de código Malicioso?		+	
¿Utiliza medida de protección de los contra código malicioso?		+	
¿Existe Manual de procedimientos documental?		+	
¿Existe manual de políticas de respaldo de la información?		+	
¿Cuenta la institución con antivirus legalizado y dentralizado?		+	

Fuente El Autor

Fuente: El Autor

ANEXO H: Lista de Chequeo

Figura 9. Lista de Chequeo 5



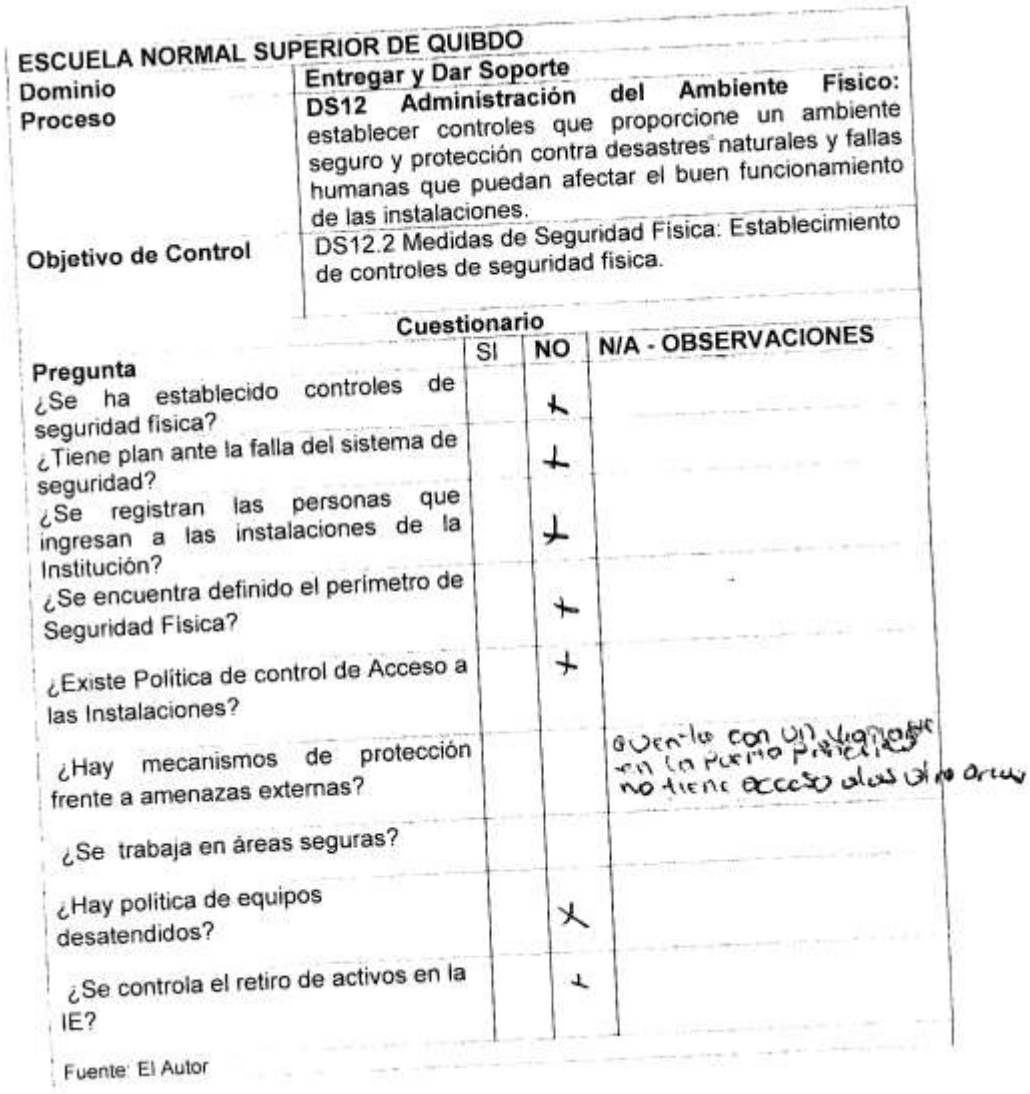
ESCUELA NORMAL SUPERIOR DE QUIBDÓ			
Dominio	**Entregar y Dar Soporte**		
Proceso	**DS5 Garantizar la seguridad de sistemas:** administrar la seguridad para proteger los activos de la institución, establecimiento de controles físicos y lógicos que permitan mejorar el buen uso de los recursos.		
Objetivo de Control	DS5.2 Plan de Seguridad de TI: Establecimiento del plan de Seguridad informática que garantice la disponibilidad, confidencialidad e integridad de la información y de la infraestructura tecnológica		
Cuestionario			
Pregunta	**SI**	**NO**	**N/A - OBSERVACIONES**
¿Cuenta la IE con política de seguridad de la información, que incluya aspectos físicos como lógicos?		X	
¿Se da a conocer la política de seguridad de la Información a los miembros de la IE?		X	
¿Se revisa las políticas para la seguridad de la información?		X	

Fuente: El Autor

Fuente: El Autor

ANEXO I: Lista de Chequeo 6

Figura 10. Lista de Chequeo 6



ESCUELA NORMAL SUPERIOR DE QUIBDO

Dominio	**Entregar y Dar Soporte**
Proceso	**DS12 Administración del Ambiente Fisico:** establecer controles que proporcione un ambiente seguro y protección contra desastres naturales y fallas humanas que puedan afectar el buen funcionamiento de las instalaciones.
Objetivo de Control	DS12.2 Medidas de Seguridad Fisica: Establecimiento de controles de seguridad fisica.

Cuestionario

Pregunta	SI	NO	N/A - OBSERVACIONES
¿Se ha establecido controles de seguridad fisica?		+	
¿Tiene plan ante la falla del sistema de seguridad?		+	
¿Se registran las personas que ingresan a las instalaciones de la Institución?		+	
¿Se encuentra definido el perimetro de Seguridad Fisica?		+	
¿Existe Politica de control de Acceso a las Instalaciones?		+	
¿Hay mecanismos de protección frente a amenazas externas?			Cuenta con un vigilante en la puerta principal no tiene acceso a las otras áreas
¿Se trabaja en áreas seguras?			
¿Hay politica de equipos desatendidos?		X	
¿Se controla el retiro de activos en la IE?		+	

Fuente: El Autor

Fuente: El Autor

ANEXO J: Lista de Chequeo 7

Figura 11. Lista de Chequeo 7

ESCUELA NORMAL SUPERIOR DE QUIBDÓ

Dominio	**Entregar y Dar Soporte**
Proceso	**DS12 Administración del Ambiente Físico:** establecer controles que proporcione un ambiente seguro y protección contra desastres naturales y fallas humanas que puedan afectar el buen funcionamiento de las instalaciones.
Objetivo de Control	DS12.4 Protección Contra Factores Ambientales: Establecer politicas de control de acceso al aula de informática para proteger contra factores ambientales.

Cuestionario

Pregunta	SI	NO	N/A - OBSERVACIONES
¿Existe detector de Humo?		X	
¿Hay control de Seguridad de acceso a lugares restringidos?		X	
¿Se ha encontrado alguna falla en el control?		X	
¿Se trabaja en áreas seguras?		X	Solo tiene una puerta de acceso
¿Existe protección del cableado de energia eléctrica y de telecomunicaciones?	X		estan en mantenimiento
¿Cuenta la sala con espacio amplio para facilitar la movilización?		X	
Existe Señalización de Zonas de Evacuación?		X	
¿Existen extintores?	X		No se conoce el uso
¿Existe Sistema de ventilación?	X		Aire acondicionado no es suficiente
¿Cuenta la institución con avisos de prohibición de fumar, comer, e ingresar liquidos a la sala?		X	
¿Se la hace seguimiento a las prohibiciones?		X	
¿Existe esquema de conexión eléctrica con interruptores?	X		Esta dentro del aula

Fuente: El Autor

Fuente: El Autor

RESUMEN ANALÍTICO ESPECIALIZADO - RAE

Tema	Evaluación del Sistema de la Infraestructura Tecnológica y Sistema de Información aplicando Procesos de Auditoria a la Institución Educativa Escuela Normal Superior de Quibdó
T**ítulo**	Auditoria Informática a la Infraestructura Tecnológica y Sistema de Información Bajo el Estándar COBIT a la Institución Educativa escuela normal superior de Quibdó.
Autores	MACHADO LLOREDA, Betty Janeth
Fuente Bibliográfica	Se referencian 12 fuentes bibliograficas, las mas mencionadas son: ESCUELA NORMAL SUPERIOR DE QUIBDÓ. Portal Institucional. Disponible en internet: < URL: http://ienormalquibdo.edu.co/portal/> ISACA. Cobit 5 Introduccion. [En Línea]. Disponible en internet: < URL: http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx> MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible en internet: < URL: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VsZ4EbbhDIU>
Año	2018
Resumen	Se realizó la auditoria en seguridad informática a la Infraestructura Tecnológica y Sistema de Información de la Institución Educativa Escuela Normal Superior de Quibdó bajo el estándar COBIT. Se evaluó la gestión administrativa de la sala de cómputo, cumplimiento de las funciones y prestación de servicios, infraestructura física, seguridad física, ubicación, infraestructura eléctrica, redes, gestión y actualización de la información, usuarios que acceden al sistema de información, utilización de la información. Se levantó la información aplicándose listas de chequeo por cada objetivo de control COBIT, mediante entrevistas y observación, se realizó el análisis de riesgos basado en la metodología MAGERIT, de identificaron activos, amenazas, valoración del riesgo, se realizaron recomendaciones frente a los hallazgos encontrados, se elaboraron propuestas de acciones preventivas y de mejora.
Palabras Claves	Auditoria, Seguridad informática, Activos, vulnerabilidades, amenazas, riesgos, análisis de riesgos, COBIT, Margerit.

Contenido

Conclusiones
Bibliografía
Anexos

Descripción del Problema

La Escuela Normal Superior de Quibdó, tiene su sistema de información e infraestructura tecnológica expuestos a la incursión de cualquier ataque; sea por virus, troyanos o hacker, hay muchos usuarios para el acceso al sistema y acceden a este desde cualquier sitio sin tener las precauciones necesarias. La falta de control y capacitación de los usuarios que acceden a la sala de informática, la falta de seguridad de la misma, el uso indebido de los recursos y la falta apropiación en materia de administración de los mismos, afectan el buen funcionamiento de los medios informáticos. De lo anterior se plantea el siguiente interrogante:

¿Cómo la auditoria informática a la infraestructura tecnológica y sistemas de información, permitirá realizar una evaluación para verificar la seguridad informática en la Institución Educativa de la Escuela Normal Superior de Quibdó?

Objetivo General

Realizar la evaluación de la seguridad informática aplicando procesos de auditoría a la infraestructura tecnológica y sistemas de información en la Institución Educativa Escuela Normal Superior de Quibdó.

Objetivos Específicos

1. Elaborar un inventario de los activos informáticos de la Escuela Normal Superior de Quibdó.
2. Realizar un diagnóstico del problema de seguridad de los elementos informáticos de la IE Escuela Normal Superior de Quibdó.
3. Realizar un análisis que permita la gestión de riesgos encontrados.
4. Proponer a la IE Escuela Normal Superior de Quibdó acciones de mejora que coadyuve con la gestión de riesgos y al mejoramiento de su seguridad.

Metodología

El proyecto de Desarrolló teniendo en cuenta las 4 fases de la auditoria en cada una se realizan una serie de actividades para dar cumplimiento a los objetivos propuestos:

Conocer el área auditada: se realizan las visitas a la institución y entrevistas al rector de la institución y al coordinador de la sala de informática los elementos a auditar son:

- **Sala de informática de la institución:** De la sala se auditará la gestión administrativa de la sala de cómputo, cumplimiento de las funciones y prestación de servicios, infraestructura física, seguridad física, ubicación, infraestructura eléctrica y redes.
- **Portal Institucional:** Gestión y actualización de la información.
- **Sistema SI3**: Usuarios que acceden al sistema y utilización de la información.

Planear la auditoría: Elaboración del plan estratégico con los pasos que se llevaran a cabo durante el proceso de auditoria teniendo en cuenta el estándar COBIT, contiene las actividades que se van a desarrollar, los responsables, fechas y recursos necesarios para la misma, Objetivo de la Auditoria, los objetivos de control COBIT.

Ejecutar la Auditoria: Identificación de riesgos teniendo en cuenta la metodología Magerit, aplicación de listas de chequeo por cada objetivos de control de Cobit seleccionados para la auditoria.

Fase de resultados: se elabora el dictamen de la auditoria teniendo en cuenta lo arrojado en la etapa de ejecución de la misma y se proponen acciones de mejora.

Referentes Teóricos y Conceptuales

La Auditoría Informática es un servicio que consisten en verificar, analizar y evaluar como una organización utiliza sus recursos informáticos y el flujo de información, como los protege y de qué

forma realiza el control y seguimiento de sus servicios, así mismo, busca identificar si existe trazabilidad en sus actividades, si cumplen adecuadamente con los fines de la organización, la normatividad y demás regulaciones.

El análisis e identificación de riesgos, ayuda a mitigar el impacto generado con la posibilidad que un riesgo ocurra, se establece controles, acciones de mejora y se emiten recomendaciones, dentro del proceso de la identificación de riesgos, es necesarios tener una metodología clara para identificar y tratar los tipos de riesgos que se puedan presentar en materia de seguridad. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, MAGERIT, pretende concientizar a la empresa de los riesgos que corre y la forma de cómo se pueden tratar de tal manera que no genere un impacto negativo a la institución. Se requiere adelantar algunos pasos fundamentales:

1. Definición de Activos: Siempre es necesario para realizar un análisis de riesgos, conocer sus activos, partiendo de un grupo que sea relevante y manejable, cada uno de esos activos deberán tener sus amenazas, las vulnerabilidades y el impacto con el que se puede analizar cada uno de los riesgos.
2. Amenazas: Son las causas potenciales que pueden generar daño en los activos, son factores externos que no se pueden controlar.
3. Vulnerabilidades: Las vulnerabilidades son las exposiciones de los activos para recibir cualquier tipo de ataque, comprometiendo así la Confidencialidad, integridad y disponibilidad, por lo que se requiere identificar las debilidades que se tiene y clasificarlas de acuerdo a una escala.
4. Salvaguardas: Las salvaguardas son todos los mecanismos existentes para reducir los riesgos.

En la actualidad la información juega un papel muy importante en cualquier empresa pública o privada, por ser el activo más importante dentro de cualquier organización, aplicando la auditoria en seguridad informática mediante COBIT ayuda a alcanzar los objetivos, además de reducir riesgos que se presentan, por no tener la institución estandarizados sus recursos tecnológicos, con sus respectivos los procesos, esto ha llevado a que se dupliquen los esfuerzos perdiendo eficacia y eficiencia, la auditoria debe proporcionar mejora en los procesos y el desarrollo de las actividades. COBIT está dividido en:

Dominios: Es una agrupación de procesos con una responsabilidad dentro de la organización.
Procesos: Conjuntos de actividades.
Actividades: Acciones para lograr un resultado.

Resultados

Con la aplicación de las listas de Chequeo del proyecto se evidenció:

- Falta de una estructura organizacional de TI, manual de funciones de la sala, donde se especifique los roles y responsabilidad de utilización de recursos, referente al sistema SI3, están definidas las responsabilidad y privilegios de acceso, pero no hay un manual que soporte, no hay inventario de activo, no cuenta con un cronograma periódico de mantenimiento de equipos preventivo y correctivo, en ocasiones son realizados por estudiantes del SENA.
- No hay plan de protección de registros, no se hace control para evitar la propagación de código malicioso, Institución no cuenta con una política de seguridad de TI, no hay controles ni plan de seguridad física, no hay registros de las personas que ingresan al aula, no está definido perímetro de seguridad física, no hay mecanismos de protección contra amenazas externas, no hay política de retiro de activos.
- No se tiene una política de control de acceso al aula de informática, no existe detector de humo, no hay zonas marcadas como restringida, el área de no se considera segura, por el momento la sala no cuenta con protección de redes eléctricas y de red, no hay fácil movilización y mucho más si las personas son discapacitados físicos, no están marcada la zona de evacuación, no tiene avisos de prohibición de fumar, comer, ingresar líquidos a la sala.

Conclusiones

En esta investigación se identificaron los elementos a auditar en la Institución Educativa, el cual contó el apoyo del rector de la Institución, Se elaboró el plan de auditoria para su posterior ejecución, se realizó primero la identificación y valoración de riesgos teniendo en cuenta la metodología Magerit, mediante las listas de chequeo se ejecutó verificando el cumplimiento de los objetivos de control de Cobit aplicables en esta auditoría, se realizó un informe con los hallazgos y recomendaciones para las directivas de la Institución.

Los resultados obtenidos en el proceso de auditoría a la infraestructura tecnológica y sistemas de información en la institución, le permitirá a las directivas diseñar e implementar un plan que involucre a toda la comunidad educativa para que se tome conciencia de la importancia de la seguridad de la información, que permita reducir el nivel de riesgo, igualmente se debe implementar un plan de protección de las instalaciones, realizar un mapa de riesgos físico, realizar señalizaciones y otros aspectos que conlleven al buen funcionamiento y uso de los recursos. Éste proyecto es les permite tener una evaluación clara del funcionamiento de sus activos informáticos y lo que se debe hacer para reducir los riesgos a los que se encuentran expuestos y así mejorar la seguridad informática de la institución.

Elaborado por:	Machado Lloreda Betty Janeth
Revisado por:	Peña Hidalgo Hernando José
Fecha Elaboración del Resumen	07/05/2018