AUDITORIA DE SEGURIDAD INFORMÁTICA PARA LA INSTITUCIÓN EDUCATIVA DEPARTAMENTAL LUIS CARLOS GALÁN - MUNICIPIO DE YACOPÍ CUNDINAMARCA

JOSÉ EDWIN GONZÁLEZ RETAMOZO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
CEAD – LA DORADA - CALDAS
2017

AUDITORIA DE SEGURIDAD INFORMÁTICA PARA LA INSTITUCIÓN EDUCATIVA DEPARTAMENTAL LUIS CARLOS GALÁN - MUNICIPIO DE YACOPÍ CUNDINAMARCA

JOSÉ EDWIN GONZÁLEZ RETAMOZO

Propuesta de grado para optar por el título de Especialista en Seguridad Informática

Asesor de Proyecto

Ing. JULIO ALBERTO VARGAS FERNÁNDEZ
Asesor de Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
CEAD–LA DORADA - CALDAS
2017

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

La Dorada Caldas, 24 de Octubre de 2017

DEDICATORIA

En primer lugar le doy gracias a Dios, ya que tú hiciste posible este sueño realidad de poder permitirme obtener el título de Especialista en Seguridad Informática. También le dedico este trabajo a mi esposa Claudia Marcela Colorado, quien estuvo a mi lado en todo este proceso, dando me fuerzas para continuar con mi formación de especialista.

Le dedico este proyecto de grado a mi familia, a mis amigos y todos los que creyeron en mí, a la universidad a la cual me ha formado con valores propios de un profesional, pero en especial se lo dedico a mi padre, quien ha estado ahí, en los momentos que lo he necesitado. Gracias, Dios los bendiga.

CONTENIDO

Página.

INTRODUCCIÓN 13

1. PLANTEAMIENTO DEL PROBLEMA 14

1.1 DESCRIPCIÓN DEL PROBLEMA 14
1.2 FORMULACIÓN DEL PROBLEMA 14

2. OBJETIVOS 15

2.1 OBJETIVO GENERAL 15
2.2 OBJETIVOS ESPECÍFICOS 15

3. JUSTIFICACIÓN 16

4. ALCANCE Y DELIMITACIÓN 17

5. MARCO DE REFERENCIA 18

5.1 ANTECEDENTES 18
5.2 MARCO TEÓRICO 19
5.2.1 Seguridad de la información. 19
5.2.2 Magerit v3.. 19
5.2.3 Análisis de riesgos informáticos.: 19
5.2.4 Metodología de análisis de riesgos. 20
5.2.5 Auditoria informática. 21
5.3 MARCO CONCEPTUAL 22
5.4 MARCO CONTEXTUAL 24
5.4.1 Reseña Histórica 24
5.4.2 Misión.. 25
5.4.3 Visión.. 26
5.5 MARCO LEGAL 27
5.5.1 La promoción y el derecho a la educación 30
5.5.2 Delitos informáticos 30
5.5.3 Metodología de análisis de gestión de riesgo 31

6. MARCO METODOLÓGICO 32

6.1 TIPO DE INVESTIGACIÓN 32
6.2 LÍNEA DE INVESTIGACIÓN 32
6.3 MÉTODO DE INVESTIGACIÓN 32
6.3.1 Objetivo 1: 32
6.3.2 Objetivo 2: 33
6.3.3 Objetivo 3: 33
6.3.4 Objetivo 4: 33
6.4 POBLACIÓN DE INVESTIGACIÓN 33
6.5 ALCANCE DE LA INVESTIGACIÓN 33

7. INFORME TÉCNICO 35

7.1 ACTIVOS DE INFORMACIÓN 36
7.1.1 Servidores y Equipos de Intercambio de Datos 37
7.1.2 Sistemas de Seguridad, Prevención y Control de Acceso 37
7.2 ETHICAL HACKING. ANÁLISIS DE VULNERABILIDADES 37
7.2.1 Evaluación de Vulnerabilidades 38
7.3 RESUMEN INFORMATIVO Y FUNCIONAL DE LOS SISTEMAS DE INFORMACIÓN SENSIBLES 41
7.3.1 GLPI. 41
7.3.2 Sistema Integrado de Matriculas SIMAT. 41
7.3.3 Sistema de Información para la Gestión Escolar (Siges). 42
7.4 RESUMEN DEL DIAGNÓSTICO DE LOS SERVICIOS MÁS RELEVANTES 43
7.5 ANÁLISIS Y EVALUACIÓN DE RIESGOS BASADO EN *MAGERIT V3* 43
7.5.1 Proceso P1: Planificación. 43
7.5.2 Proceso P2: Análisis de riesgos. 45
7.5.3 Proceso P3: Estimación del estado de riesgo. 81
7.6 HALLAZGOS ENCONTRADOS 83
7.7 CONTROLES 85
7.7.1 Mecanismos de control de activos 87
7.8 RESUMEN DE CONTROLES 91

8. PRESENTACIÓN DE INFORME Y RESULTADOS FINALES 93

8.1 RECURSO AUDITADO HARDWARE 93
8.1.1 Situación 93
8.2 RECURSO AUDITADO SOFTWARE 94
8.3 RECURSO AUDITADO REDES 95
8.4 RECURSO AUDITADO INSTALACIONES FÍSICAS 96
8.5 RECURSO AUDITADO SEGURIDAD INFORMÁTICA 96

9. POLÍTICAS DE SEGURIDAD INFORMÁTICA 98

9.1 SEGURIDAD RELACIONADA AL PERSONAL 99
9.1.1 Funcionarios 99
9.1.2 Capacitación 99
9.1.3 Incidentes y atención a los usuarios 100
9.1.4 Seguridad lógica. 101
9.1.5 Control de acceso 101
9.1.6 Administración de acceso de usuarios 101
9.1.7 Uso de contraseñas. 102
9.1.8 Responsabilidades de los usuarios 103
9.1.9 Uso del correo electrónico 103

10. ESTRATEGIAS DE DIVULGACIÓN DEL PROYECTO 104

11. CONCLUSIONES 105

12. RECOMENDACIONES 106

BIBLIOGRAFÍA 107

ANEXOS 112

LISTA DE FIGURAS

Página.

Figura 1. Estructura de *MAGERIT* 21

Figura 2. Estructura Organizacional 26

Figura 3. Ministerio de Educación Nacional 42

Figura 4: Sistema de Información para la Gestión Escolar 42

Figura 5. Análisis de riesgos 45

Figura 6. Dependencia de activos tipo aplicación informática 47

Figura 7. Dependencia de los activos del tipo de servicio 47

Figura 8. Dependencia de activos del tipo equipamiento informático 48

Figura 9. Dependencia de activos tipo aplicaciones informáticas 48

Figura 10. Dependencia de los activos del tipo de comunicaciones 49

Figura 11: Los activos que son soportados por el tipo de activo personal. 49

Figura 12. Los activos que soportan por el tipo de activos equipamiento informático. 50

Figura 13: Los activos que son soportados por el tipo de activos equipamiento auxiliar. 51

Figura 14. Los activos que son soportados por el tipo de activos instalaciones. 52

Figura 15. Los activos que son soportados por el tipo de activos aplicaciones. 53

Figura 16. Valoración suplantación de identidad 85

LISTA DE TABLAS

Página.

Tabla 1. Activos 46

Tabla 2. Valoración de activos tipo: Aplicaciones 54

Tabla 3. Valoración de Activos Tipo Servicios 55

Tabla 4. Valoración de Activos Tipo: Redes de Comunicaciones 57

Tabla 5. Valoración de Activos Tipo: Equipamiento Informático 57

Tabla 6: Valoración de Activos Tipo: Equipamiento Auxiliar 59

Tabla 7. Valoración de Activos Tipo: Personal 59

Tabla 8. Valoración de Activos Tipo: Instalaciones 60

Tabla 9. Frecuencia de amenazas 61

Tabla 10. Degradación de las amenazas 61

Tabla 11. Valoración de Amenazas Tipo: Aplicaciones Informáticas 62

Tabla 12. Identificación y valoración de amenazas: Servicios. 63

Tabla 13. Identificación y valoración de amenazas: redes de comunicaciones 64

Tabla 14. Identificación y valoración de amenazas: Equipamiento informático. 65

Tabla 15. Identificación y valoración de amenazas: Equipamiento auxiliar 66

Tabla 16. Identificación y valoración de amenazas: Instalaciones 66

Tabla 17. Identificación y valoración de amenazas: Personal 67

Tabla 18. Salvaguarda activos: protecciones generales u horizontales 68

Tabla 19. Salvaguardas activos: Protección de los datos/información 68

Tabla 20. Salvaguarda activos: Protección de los servicios 69

Tabla 21. Salvaguardas activos: Protección de las aplicaciones (Software) 70

Tabla 22. Salvaguarda activos: Protección de los equipos (Hardware) 70

Tabla 23. Salvaguardas activos: Protección de las comunicaciones. 71

Tabla 24. Identificación de amenazas 71

Tabla 25. Valoración de amenazas de cada uno de los activos 75

Tabla 26. Impacto potencial sobre cada uno de los activos 81

Tabla 27. Impacto potencial sobre cada uno de los activos 82

Tabla 28. Clasificación de controles 91

Tabla 36. : Pregunta 1 encuesta 116

Tabla 37: Pregunta 2 encuesta 117

Tabla 38: Pregunta 3 encuesta 118

Tabla 40: Pregunta 4 encuesta 119

LISTA DE CUADROS

Página.

Cuadro 1: Evaluación de vulnerabilidades 38

Cuadro 2: Criterios de evaluación 53

Cuadro 3: Degradación del valor 74

Cuadro 4: Probabilidad de ocurrencia……....74

LISTA DE ANEXOS

Página.

ANEXO A. Clasificación de los activos…… 113

ANEXO B. Encuesta aplicada……. 115

ANEXO C. Autorización auditoria institución…….. 115

INTRODUCCIÓN

Los avances en el desarrollo de la tecnología, como también en materia de la sistematización de datos, han llevado a que las instituciones educativas implanten modelos de gestión de información en sus sedes; llevando así a que se realice una auditoría de seguridad informática para valorar la forma en que se venían archivando los documentos de las diferentes actividades que se realizan en la institución, relacionadas con el procesamiento y manejo de información de las calificaciones de los alumnos en la Institución Luis Carlos Galán, con el fin de implementar un sistema de seguridad informática que protejan las posibles amenazas y vulnerabilidades que se puedan presentar; beneficiando a todos los usuarios en la parte administrativa, alumnos, ex alumnos, docentes y comunidad en general.

De acuerdo con el método de observación realizada, se determinaron procedimientos para poder realizar la sistematización de los procesos que se están llevando en la institución de forma segura y garantizando la seguridad los recursos de información.

Por esta razón se realizará una auditoria a la seguridad del sistema de información, determinando el estado actual de la institución y estableciendo los mecanismos a realizar.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCIÓN DEL PROBLEMA

Al realizarse la auditoria a la seguridad del sistema de información, se podrán identificar diferentes tipos de riesgos, vulnerabilidades, fallas y amenazas, que puedan presentarse en la institución, llevando a implementar medidas de corrección y políticas de seguridad.

La Institución Educativa Departamental Luis Carlos Galán, maneja una base de datos de los alumnos matriculados, que es llevado en la plataforma SIMAT, que es administrada por la Secretaria de Educación Nacional, y para el manejo de registro de notas, se realiza con otra plataforma llamada SIGES, que es administrada por la secretaria de educación de Cundinamarca; este último, ha tenido en sus últimos años dificultades con su sistema de información de registro de notas, como por la suplantación de usuarios al sistema.

La institución educativa departamental Luis Carlos Galán, del municipio de Yacopí Cundinamarca, cuenta con 24 sedes en áreas rurales del municipio, encontrándose distantes a la sede principal y en zonas de difícil acceso.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo la auditoria del Sistema de gestión de seguridad de la información ayudará a disminuir las vulnerabilidades y amenazas de seguridad en el registro académico y de notas de los estudiantes en la institución educativa departamental Luis Carlos Galán del municipio de Yacopí – Cundinamarca?

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Disminuir las vulnerabilidades y amenazas de seguridad en el registro académico y de notas de los estudiantes con la auditoria del sistema de gestión de seguridad de la información para la institución educativa departamental Luis Carlos Galán del municipio de Yacopí – Cundinamarca.

2.2 OBJETIVOS ESPECÍFICOS

Para llevar a cabo la ejecución de este proyecto se deben tener en cuenta los siguientes criterios:

- Realizar un levantamiento de información del estado actual de la institución educativa departamental Luis Carlos Galán.

- Elaborar un plan de auditoría de acuerdo a la información recolectada.

- Realizar las respectivas recomendaciones de acuerdo a los resultados obtenidos de la auditoria.

- Realizar un informe de auditoría para la institución educativa.

3. JUSTIFICACIÓN

La Institución Educativa Departamental Luis Carlos Galán, del Municipio de Yacopí Cundinamarca, ha venido progresivamente registrando su información de acuerdo con sus capacidades tecnológicas.

La información llevada por la institución es importante, ya que con ella se tiene un historial de los estudiantes que están o estuvieron registrados en la institución, certificándoles sus estudios para la nación.

Esta información puede encontrarse vulnerada y adulterada, para quienes de manera inadecuada lo utilice para su propio bien.

La auditoría informática es uno de los aspectos más importantes en la investigación de los dispositivos informáticos de una institución, ofreciendo herramientas para la seguridad en los sistemas y estableciendo políticas, de modo que determine qué es lo que se está haciendo mal y corregirlo; brindando a la comunidad educativa un mejor servicio en los procesos pedagógicos pertinentes.

Por esta razón la institución deberá implementar una auditoria al sistema de seguridad informático e implementar un plan de mejoramiento.

4. ALCANCE Y DELIMITACIÓN

La Auditoria se llevará a cabo a la Seguridad del Sistema de Información de la Institución Educativa Departamental Luis Carlos Galán del Municipio de Yacopí Cundinamarca, permitiendo establecer las amenazas, riesgos, vulnerabilidades y fallas que se estén presentando. Para después elaborar un informe, describiendo el plan de mejoramiento a implementar con las políticas de seguridad.

5. MARCO DE REFERENCIA

5.1 ANTECEDENTES

Las normas en seguridad informática como la ISO 27000 se han generado a partir de entes normalizadores británicas como lo es la (British Standards Institution) que divulgaron documentos sobre prácticas en Seguridad para empresas desde 1995, a partir de este momento se empezó a crear la familia 27000 siendo como requisito para un Sistema de gestión de la seguridad de Información o SGSI, que puede ser aplicado de manera internacional, de esta manera se siguen gestando nuevos complementos como la norma ISO 17000.

Se han desarrollado diferentes estudios e investigaciones sobre seguridad informática, así mismo se han realizado proyectos de grado relacionados con el tema. Como lo puede ser la auditoria en seguridad en informática para una empresa específica, universidades e instituciones educativas; donde se encuentran políticas de seguridad y diferentes métodos de detección y ataques a sistemas informáticos.

Juan David Vargas Gutiérrez, en su proyecto de grado para optar por el título de tecnología en sistemas, diseño de un sistema de calificaciones web para el colegio Alto Sumisa de puente nacional Santander, de la universidad nacional abierta y a distancia (UNAD), en el programa. Con el fin de diseñar un sistema de calificaciones. Proporcionando para el proyecto, el agilizar los procesos, tratamiento e integridad de los datos[1].

Jorge Luis Galeano Villa y Cristian Camilo Álzate Castañeda, en su proyecto de Protocolo de políticas de seguridad informática para las universidades de Risaralda; para optar por el título de ingeniería de sistemas y telecomunicaciones, de la universidad católica de Pereira, proponiendo pautas claras al momento de implementar la seguridad, proporcionando una orientación y unas recomendaciones en la elección de herramientas. Siendo de gran aporte para la realización del proyecto al momento de aplicar una auditoria[2].

[1] VARGAS GUTIÉRREZ, Juan David. Tecnología en sistemas, diseño de un sistema de calificaciones WEB para el Colegio Alto Semisa. Puente Nacional (Santander): Universidad Abierta y a Distancia –UNAD- 2013, p. 108

[2] GALEANO VILLA, Jorge Luís y ÁLZATE CASTAÑEDA, Cristian Camilo. Protocolo de políticas de seguridad informática para las universidades de Risaralda. Pereira: Universidad Católica, 2013, p. 100

5.2 MARCO TEÓRICO

5.2.1 Seguridad de la información. Es un término que hace referencia a la seguridad de activos de forma general, incluyendo la seguridad informática, la seguridad TIC y la seguridad de los datos. Los cuales se ocupan a diseñar normas, procedimientos, métodos y técnicas. Consiguiendo un sistema de información segura y confiable.

La seguridad de la información, es la protección total al sistema, pero garantizarla es imposible[3], ya que no existe un sistema cien por ciento seguro. La vulnerabilidad en el sistema, el peligro o el daño de la misma pueden afectar en sí la esencia de la información, obteniendo resultados defectuosos al momento de una consulta o la administración de ésta.

Las organizaciones y sus sistemas de seguridad de la información, se encuentran adoptando como parte de su misión y visión, normas o metodologías, que minimicen los riesgos e inseguridades como fraudes, espionaje, sabotaje, vandalismo, incendios o inundaciones; y maximizando las inversiones y las oportunidades. Estos ataques se están volviendo más comunes.

La información es el activo más importante para las organizaciones, tanto para el sector público como el privado, siendo para ambas el común denominador, como también la parte más vulnerable en la mayoría de los sistemas informáticos, ya que no han sido diseñados para ser seguros.

5.2.2 *Magerit v3.* Metodología de análisis y gestión de riesgos desarrollada por el consejo superior de administración electrónica, que es utilizada para disminuir los riesgos cuando son implementamos en el uso de las tecnologías de la información. La metodología MAGERIT se destaca en analizar el impacto que puede provocar a una empresa la violación de seguridad; identificando las amenazas y vulnerabilidades para crear medidas preventivas y correctivas más apropiadas; presentando una guía completa paso a paso de cómo llevar a cabo el análisis de riesgos.

5.2.3 Análisis de riesgos informáticos. A continuación se define lo que es un riesgo, para poder definir lo que es el análisis de riesgos:

[3] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 2700. Sistema de gestión de seguridad de la información. Términos de uso información. 2012. [on line], [consultado el 3 de septiembre de 2017]. Disponible en internet: www.iso27000.es/iso27000.html

Según Fernando Izquierdo Duarte[4]: "El riesgo es un incidente o situación, que ocurre en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias negativas o positivas que podrían afectar el cumplimiento de los objetivos".

Según Alberto Cancelado González: "El riesgo es una condición del mundo real en el cual hay una exposición a la adversidad, conformada por una combinación de circunstancias del entorno, donde hay posibilidad de perdidas"[5].

Según Martin Vilches Troncoso[6]: "El riesgo es cualquier variable importante de incertidumbre que interfiera con el logro de los objetivos y estrategia del negocio. Es decir es la posibilidad de la ocurrencia de un hecho o suceso no deseado o la no-ocurrencia de uno deseado".

Ya aclarado el concepto de riesgo, se establece el concepto de análisis de riesgos, siendo este el más importante en la gestión de la seguridad de la información, estableciendo estrategias en la toma de decisiones de los riesgos, eliminándolos, ignorándolos, mitigarlos y controlarlos; esta gestión de riesgo se basa en determinar, analizar, evaluar y clasificar los activos de información más importantes.

Para establecer un análisis de riesgos, se deben tener claros los objetivos y una escala valorativa con cierta regla de priorización de los mismos; para después condensar en una matriz, donde se muestre el nivel de impacto según la escala valorativa, estableciendo el estado actual en materia de seguridad de la información.

5.2.4 Metodología de análisis de riesgos. La metodología de análisis de riesgos, son implementadas para la identificación de controles y estableciendo medidas para estas vulnerabilidades. La metodología de análisis de riesgos se clasifican en dos: Las cuantitativas y las cualitativas.

---

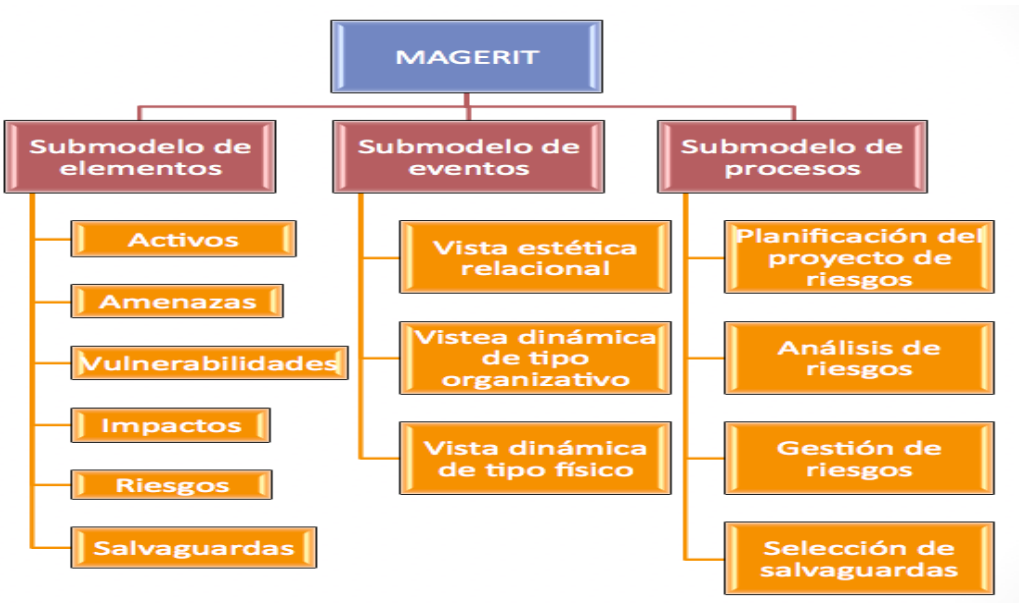
[4] IZQUIERDO D, Fernando. La administración y los riesgos. [en line]. EN: Maxitana C, Jennifer D. (Auditor en control de gestión). Tesis: Administración de riesgos de tecnología de información de una empresa del sector informático. Guayaquil – Ecuador: Escuela Superior politécnica del Litoral, 2005. p.39. [on line], [consultado el 3 de septiembre de 2017]. Disponible en internet: http:// www.cib.espol.edu.ec/Digipath/D_Tesis_PDF/D-33960.pdf

[5] CANCELADO GONZÁLEZ, Alberto. El riesgo es una condición del mundo real en el cual hay una exposición a la adversidad. [on line], [consultado el 3 de septiembre de 2017]. Disponible en internet: stadium.unad.edu.co/preview/UNAD. php?url=/bitstream/ 10596/2655/3/76327474.

[6] VILCHES T, Martín. El riesgo [en line]. En: Machuca C, John. (Magister en Contabilidad y Auditoría). Tesis Guía para la evaluación del sistema de riesgo operativo en la Cooperativa de Ahorro y Crédito Jardín Azuayo. Cuenca – Ecuador. Universidad de Cuenca, 2011. p.21. [on line], [consultado el 3 de septiembre de 2017]. Disponible en internet: http://dspace.ucuenca.edu. ec/ bitstream/123456789/2729/1/tm4487.pdf

Para la realización de este proyecto se adoptará una metodología, que es la *MAGERIT v3* (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información); dentro de esta metodología se encuentra un esquema completo de etapas, actividades y tareas del sud-modelo de procesos *MAGERIT*[7], en donde se determina cual puede aplicarse en su totalidad, dependiendo del proyecto.

Figura 1. Estructura de *MAGERIT*



Fuente: (Infotegra.com, 2017)

5.2.5 Auditoria informática. La auditoría informática se define como un examen metódico, puntual y discontinuo que verifica y evalúa; destinada a la ayuda en la mejora de la seguridad, eficacia, eficiencia y rentabilidad de los sistemas de información de la organización, establece en opinión objetiva fundada en las evidencias, con unos objetivos muy concretos; mejorar la eficacia en la organización de los sistemas de información, para proteger los activos y recursos; garantizando resultados fiables en el tiempo, costos y utilidad. Mejorar los procedimientos, estándares y planificación colaborando en su diseño y en la actualización de sus normas.

Las fases que debe llevar una auditoria informática son cinco:

[7] BOLAÑOS, María C y ROCHA G. Mónica. 25 de marzo de 2014. Auditoria de SI. MageritV3 (Metodología de Análisis y Gestion de Riesgos de los Sistemas de Información). [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: http://asijav.weebly.com/auditoria-de-sistemas-de-informacioacuten/magerit-v3-metodologa-eanlisis-y-gestin-de-riesgos-de-los-sistemas-de-informacion.

- El proceso de inicio: es la toma de contacto entre el auditor o el equipo auditor y la empresa; hay una formalización contractual mediante un contrato se establecen una serie de normas. Es necesario identificar al interlocutor válido por parte de la empresa a auditar o del servicio a auditar que generalmente coincide con el máximo responsable. La definición del alcance y el objetivo de la auditoria, la confección del plan de trabajo a desarrollar.

- El desarrollo de trabajos: es la recopilación de la información, por medio de entrevistas, revisión de documentos, pruebas y verificación de datos; en definitiva trabajos de campo.

- Evaluación de la información: es la síntesis y análisis de los datos recopilados, como previsión, comprobación, cumplimiento de normas, estándares, seguimientos y estándares reconocidos. Todo este análisis debe estar justificado con evidencias.

- Presentación de resultados: el informe de auditoría es la presentación de los resultados obtenidos, es recomendable mantener reuniones para la presentación de un borrador de informe y permitir a la entidad o a la organización en un plazo prefijado observaciones y alegaciones a ese borrador, que serán estudiadas por el equipo o por el auditor a presentar el informe definitivo.

- Redacción del informe de auditoría: es la presentación del informe de auditoría, señalando que las recomendaciones deben ser llevadas a cabo en un periodo de tiempo determinado, las recomendaciones son soluciones a los problemas detectados basadas en experiencia del auditor, no son ejecutivas. Este informe de auditoría debe contener título, índice, introducción, objetivos y alcance, metodología, resultados, las alegaciones de los auditados, anexos, fechas de emisión y de entrega, conclusiones y las recomendaciones.

5.3 MARCO CONCEPTUAL

A continuación se hacen definiciones asociadas a la seguridad informática, que serán utilizados en el desarrollo de éste proyecto:

Activos informáticos: Son todos los elementos o recursos (hardware y software) que posee una empresa, es decir, todo elemento que compone el proceso completo de comunicación, como por ejemplo: servidores, bases de datos, *routers,* etc.

Seguridad de la información: Consiste en crear un conjunto de medidas preventivas y reactivas de las organizaciones, sirviendo de protección de la información, en contra de amenazas y peligros, evitando daños y minimizando riesgos; garantizando su confidencialidad, integridad y disponibilidad.

Confidencialidad: Son los datos que son protegidos durante el intercambio de información entre el emisor y el destinatario, donde solo pueden ser legibles y modificados por los usuarios autorizados.

Integridad: Hace referencia a mantener la propiedad de los datos sin modificaciones no autorizadas

Disponibilidad: Es la condición de encontrarse la información a disposición de los usuarios autorizados a acceder a ella.

Vulnerabilidad: Se define como las debilidades de un sistema comprometiendo la seguridad del sistema informático.

Amenazas: Se define como eventos o acciones que pueden causar daño al sistema de información.

Riesgos: Se define como la exposición a adversidad como atentados y amenazas a los sistemas informáticos.

Ataque: Se define como las amenazas que se han convertido en realidad, causando daños en los activos.

Autenticidad: Se define aquella información legítima y acreditable de una persona, servicio o elementos que debe ser comprobable.

Auditoria: Proceso que tiene como fin recoger, agrupar y evaluar un sistema de información, analizando la eficiencia, el cumplimiento de la normatividad, entre otros.

Bases de datos: Es un conjunto de datos organizados y relacionados entre sí. De tal forma que se pueda organizar para poder consultar y utilizar fácilmente.

Controles: Métodos, sistemas y procedimientos, que en forma ordenada, se adoptan en una organización, para asegurar la protección de todos sus recursos[8]

MAGERIT: Metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España[9]

[8] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Op. Cit.p. 16

Norma ISO: La ISO (International Standarization Organization), como su nombre lo indica es la organización encargada de la normalización o estandarización de normas de tal forma que puedan ser aplicadas a nivel internacional obteniendo efectividad en los procesos y reducción de los costos asociados[10].

Salvaguarda: Medida de protección que garantiza la disminución de un riesgo (*Magerit* Libro I, 2012, p. 19).

Seguridad Informática: Área de la informática que se encarga de la protección y la privacidad de la información, comprendiendo software y hardware por medio de normas, procedimientos, métodos y técnicas.

SGSI: Sistema de Gestión de la Seguridad de la Información. Conjunto de políticas para el diseño, implementación y mantenimiento de los controles necesarios para garantizar la seguridad de la información minimizando los riesgos a los que está expuesta[11]

5.4 MARCO CONTEXTUAL

5.4.1 Reseña Histórica. La Institución Educativa Departamental LUIS CARLOS GALÁN, se encuentra ubicada en el municipio de Yacopí, departamento de Cundinamarca, Inspección de Terán, Km 30 vía a La Dorada Caldas. Es la parte sur oriental del municipio, con clima Caliente apto para la ganadería y gran variedad de cultivos, donde sobresale especialmente la Ganadería.

La institución LUIS CARLOS GALÁN fue creada en el año 2002 atendiendo a los requerimientos fijados por el Ministerio de Educación Nacional en su Decreto 1494 del 19 de Julio 2002.

El 30 de Septiembre del 2002. La Secretaria Departamental de Educación de Cundinamarca mediante Resolución N º 3365, en la cual da marco legal a las Instituciones.

La Institución LUIS CARLOS GALÁN, está conformada por veintidós (22) sedes ubicadas geográficamente en la Inspección de Bilbao de Terán, Patevaca, Castillo

---

[9] SUAREZ, P. Análisis y diseño de un sistema de gestión de seguridad informática. 2013, p.45. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: stadium.unad. edu.co/ preview/ UNAD.php?url=/bitstream/10596/3777/1/20904541.

[10] Ibíd.,p. 28

[11] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Op.cit.p. 20

y Guayabales, las cuales ofrecen los servicios de grados Preescolar hasta el grado Quinto (5º) , una (1) en Básica Académica y dos (2) Básica Secundaria.

Centros Educativos

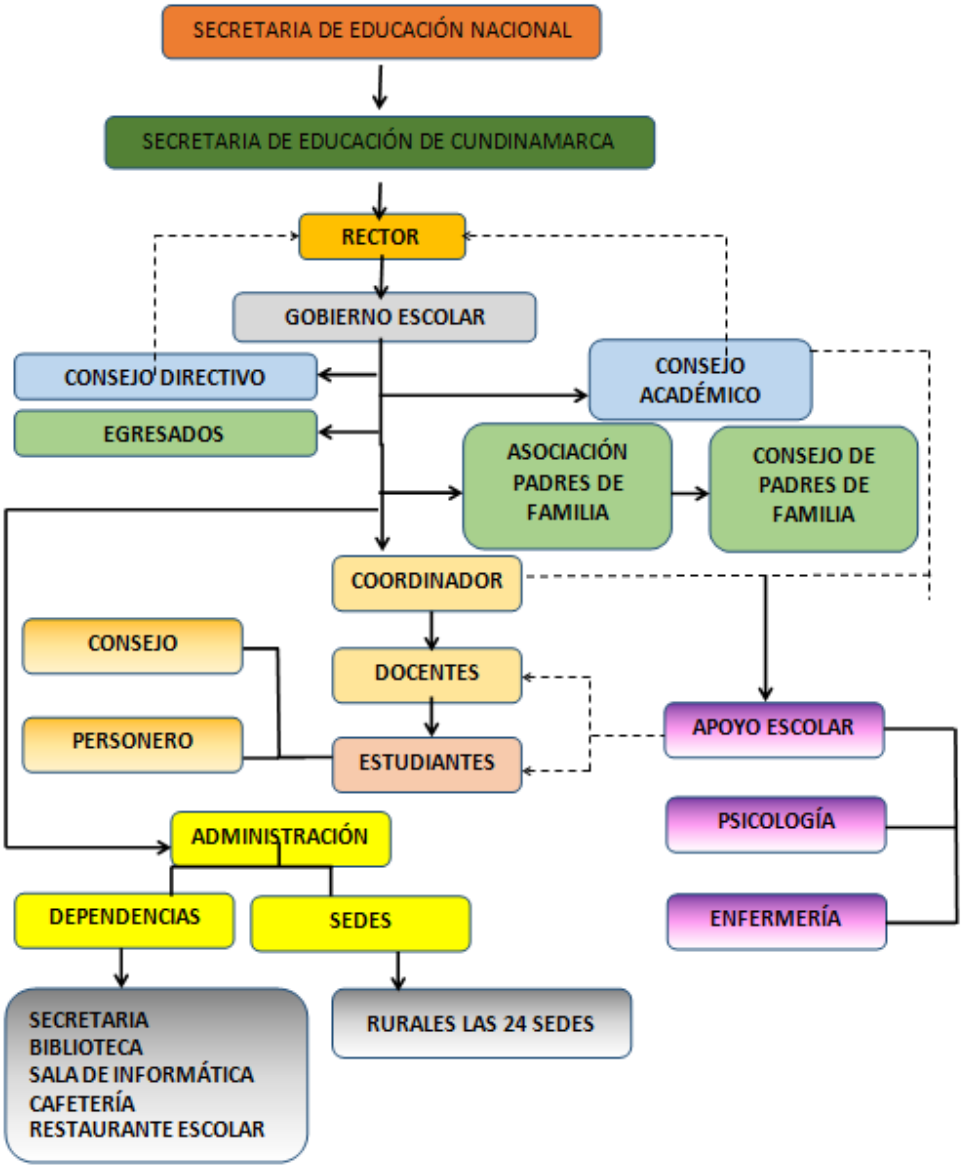
- Colegio Terán, LUIS CARLOS GALÁN (Sede Principal)
- Colegio Guayabales
- Colegio Patevaca
- Colegio el Castillo
- Sede La collareja.
- Sede Los Almendros.
- Sede La Istapa.
- Sede Caño Hondo
- Sede Nacopaicito.
- Sede La Tórax.
- Sede Guayabales.
- Sede La Balanza.
- Sede La Muñoz,
- Sede Unidad Básica Bilbao de Terán.
- Sede Campo Alegre.
- Sede la Oscura
- Sede Unidad Básica el Castillo.
- Sede Morro Pelao.
- Sede Ventanas.
- Sede el Clavijo.
- Sede Nacederos.
- Sede Caipal.

5.4.2 Misión. La Institución Educativa Departamental Luis Carlos Galán del municipio de Yacopí, tiene como misión, garantizar la prestación del servicio educativo en los niveles de preescolar, primaria, secundaria y media académica con énfasis en técnico en sistemas articulado con el SENA, ofreciendo calidad, cobertura y eficacia, a través de un currículo pertinente, para la formación integral del hombre y la mujer en la jurisdicción de las inspecciones de: Guayabales, Patevaca y Terán, promoviendo los valores como principios de formación y estimulación del desarrollo tecnológico de la comunidad escolar, la cual está llamada a transformar para su bienestar y el de los demás.

5.4.3 Visión. En el año 2018 el I.E.D Luis Carlos Galán del municipio de Yacopí, será un plantel caracterizado por brindar educación de calidad de acuerdo a las nuevas políticas educativas, utilizando las nuevas tecnologías, formando seres humanos competentes con principios y valores.

5.4.4 Estructura Organizacional

Figura 2. Estructura Organizacional



Fuente: IED Luis Carlos Galán

5.5 MARCO LEGAL

Para una visión global del marco legal y su aplicabilidad real a las necesidades del perfil Galanista, se hace necesario tener en cuenta las siguientes sentencias de la Corte Constitucional.

- Al interpretar el artículo 16 de la Constitución que consagra el derecho al libre desarrollo de la personalidad, la corte constitucional y la doctrina han entendido que:

> "Ese derecho consagra una protección general de la capacidad que la Constitución reconoce a las personas para auto determinarse, esto es, a darse sus propias normas y desarrollar planes propios de vida, siempre y cuando no afecten derechos de terceros."[12]

- Que "Al momento de matricularse una persona en un Centro Educativo celebra por ese acto un Contrato de Naturaleza Civil; un contrato es un acuerdo de voluntades para crear obligaciones"[13].

- Que:

> "La exigibilidad de esas reglas mínimas al estudiante resulta acorde con sus propios derechos y perfectamente legítima cuando se encuentran consignadas en el Manual de Convivencia que él y sus acudientes, firman al momento de establecer la vinculación educativa. Nadie obliga al aspirante a suscribir ese documento, así como a integrar el plantel, pero lo que sí se le puede exigir, inclusive mediante razonables razones es que cumpla sus cláusulas una vez han entrado en Vigor, en este orden de ideas, concedida la oportunidad de estudio, el comportamiento del estudiante si reiteradamente incumple pautas mínimas y denota desinterés o grave indisciplina puede ser tomado en cuenta como motivo de exclusión"[14].
>
> "La Corte Constitucional ha reiterado a lo largo de la jurisprudencia, en el sentido de considerar que quien se matrícula en un Centro Educativo, con el objeto de ejercer el derecho Constitucional fundamental que lo ampara, contrae por ese mismo hecho obligaciones que debe cumplir, de tal manera

[12] CORTE CONSTITUCIONAL. Sentencia C-481/98. Régimen disciplinario para docente. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: www.corteconstitucional.gov.co/ relatoria/1998/c-481-98.htm

[13] CORTE CONSTITUCIONAL. T-612/92. Derecho a la educación. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: www.corteconstitucional.gov.co/relatoria/1992/T-612-92.htm

[14] CORTE CONSTITUCIONAL. Principio de primacía de realidad sobre formalidades establecidas por sujetos de relaciones laborales/relación de trabajo

que NO puede invocar el mencionado derecho para excusar las infracciones en que incurra."[15]

- Que:

"La Educación surge como un derecho – deber que afecta a todos los que participan en esa órbita cultural respecto a los derechos fundamentales, no sólo son derechos en relación a otras personas, sino también deberes de la misma persona para consigo misma, pues la persona no sólo debe respetar el ser personal del otro, sino que también ella debe respetar su propio ser."[16]

- Que:

"La Educación sólo es posible cuando se da la convivencia y si la disciplina afecta gravemente a ésta última, ha de prevalecer el interés general y se puede ir respetando el debido proceso, separar a la persona del establecimiento Educativo. Además, la permanencia de la persona en el sistema educativo está condicionada por su concurso activo en la labor formativa; la falta de rendimiento intelectual también puede llegar a tener suficiente entidad como para que la persona sea retirada del establecimiento donde debía aprender y no lo logra por su propia causa"[17].

- Que:

"La educación ofrece un doble aspecto. Es un derecho-deber, en cuanto no solamente otorga prerrogativas a favor del individuo, sino que comporta exigencias de cuyo cumplimiento depende en buena parte la subsistencia del derecho, pues quien no se somete a las condiciones para su ejercicio, como sucede con el discípulo que desatiende sus responsabilidades académicas o infringe el régimen disciplinario que se comprometió observar, queda sujeto a las consecuencias propias de tales conductas: la pérdida de las materias o la imposición de las sanciones previstas dentro del régimen interno de la

[15] CORTE CONSTITUCIONAL. Sentencia T-**235/97**. Derecho a la educación. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: www.corteconstitucional.gov.co/ relatoria/1997/t-235-97.htm

[16] CERCA DE PIEDRA. ST- 02/92: Manual de convivencia. 2016. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: www.cercadepiedra.edu.co/ images/.../MANUAL_DE_ CONVIVENCIA_2016.

[17] CORTE CONSTITUCIONAL. Sentencia No. T-**316/94**. Derecho a la educación/plantel educativo. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: www.corteconstitucional. gov.co/relatoria/1994/T-316-94.htm

institución, la más grave de las cuales, según la gravedad de la falta, consiste en su exclusión del establecimiento educativo"[18].

- Que:

  "La función social que cumple la Educación hace que dicha garantía se entienda como un derecho – deber que genera para el Educador como para los educandos y para sus progenitores un conjunto de obligaciones recíprocas que no "establecer una serie de normas o reglamentos en donde se viertan las pautas de comportamiento que deben seguir las partes del proceso Educativo"[19].

- Que:

  "Las instituciones educativas pueden regular el uso del teléfono celular dentro de las instalaciones, incluyendo la reglamentación correspondiente en el manual de convivencia, el cual establecerá en forma clara su utilización, sin llegar a prohibirlo, así como las sanciones y el procedimiento a aplicar en caso de infracciones".[20]

  El hombre, considera la Corte constitucional, debe estar preparado para vivir en armonía con sus congéneres, para someterse a la disciplina que toda comunidad supone, para asumir sus propias responsabilidades y para ejercer la libertad dentro de las normas que estructuran el orden social. Así pues, de ninguna manera ha de entenderse completo ni verdadero un derecho a la educación al que se despoja de estos elementos esenciales, reduciéndolo al concepto vacío de pertenencia a un establecimiento educativo…

- "…De lo dicho se concluye que cuando el centro educativo exige del estudiante respuestas en materia académica, disciplinaria, moral o física, o cuando demanda de él unas responsabilidades propias de su estado, así como cuando impone sanciones proporcionales a las faltas que comete, siempre que desempeñe tal papel de modo razonable y sujeto al orden jurídico, no está violando los derechos

[18] CORTE CONSTITUCIONAL. Sentencia No. T-519/92. Derecho a la educación. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: www.corteconstitucional.relatoria/1992/T-519-92.htm

[19] CORTE CONSTITUCIONAL. T-527/95. Derecho a la educación. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: www.corteconstitucional.gov.co/relatoria/1995/t-527-95.htm

[20] CORTE CONSTITUCIONAL. Sentencia T-967 de 2007: Derecho a la educación frente a derechos económicos. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: www.corteconstitucional.gov.co/relatoria/2007/t-967-07.htm

fundamentales del educando sino, por el contrario, entregando a éste la calidad de educación que la constitución desea"[21]

5.5.1 La promoción y el derecho a la educación

- No se vulnera el derecho a la Educación por pérdida del año[22].
- No se vulnera el derecho a la Educación por sanciones al mal rendimiento[23].
- No se vulnera el derecho a la Educación por normas de rendimiento y disciplina[24]
- No se vulnera el derecho a la Educación por la exigencia al buen rendimiento[25]
- No se vulnera el derecho a la Educación por expulsión debido al mal rendimiento o faltas de disciplina[26]

5.5.2 Delitos informáticos

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"[27]

[21] CORTE CONSTITUCIONAL. Sentencia T-397/97. Igualdad de derechos entre cónyuge y compañera permanente. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: www.corteconstitucional.gov.co/relatoria/1997/T-397-97.htm

[22] CORTE CONSTITUCIONAL. ST 098 3/03/94: Nuevo Manual de Convivencia. 2015. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: manualmepalumnos. blogspot. com/2011/03/nuevo-manual-de-convivencia-2011.

[23] CORTE CONSTITUCIONAL. ST 596 7/12/94: Sentencias y documentos de apoyo frente a las normas y manuales del colegio. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: https://www.facebook.com/notes/gestioncomunitaria.../320232048043712/

[24] CORTE CONSTITUCIONAL. ST 316 12/06/94 Op. Cit. p.16

[25] CORTE CONSTITUCIONAL. ST 439 12/10/94: falta de rendimiento académico.

[26] Ibíd., p. 27

[27] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS TELECOMUNICACIONES. Ley 1273 de 2009. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-3705.html

5.5.3 Metodología de análisis de gestión de riesgo

MAGERIT: Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno.[28]

[28] ADMINISTRACIÓN ELECTRÓNICA. ST 098 3/03/94: Magerit v3. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: http:// administracionelectronica.gob.es/pae_Home/ pae_ Documentacion/ pae_ Metodolog/pae_Magerit.html#.VCmVZhZRVJQ

6. MARCO METODOLÓGICO

6.1 TIPO DE INVESTIGACIÓN

Para la realización de este proyecto se tuvo en cuenta el tipo de investigación formativa establecida en el reglamento de investigación de la Universidad Nacional Abierta y a Distancia UNAD, pretendiendo aplicar los conocimientos adquiridos durante la formación académica.

6.2 LÍNEA DE INVESTIGACIÓN

La escuela ECBTI (Escuela de Ciencias Básicas, Tecnología e Ingeniería), maneja unas líneas de investigación para el desarrollo de los proyectos, el cual se aplicara para la elaboración de éste. El tipo de investigación a utilizar es ***cuantitativo*** de carácter exploratorio, para producir una lista de riesgos y así compararlas entre sí con facilidad por tener asignados unos valores numéricos, determinando la probabilidad de ocurrencia de un evento.

6.3 MÉTODO DE INVESTIGACIÓN

A continuación se define los pasos a seguir en la investigación, determinando así los objetivos propuestos en el proyecto:

6.3.1 Objetivo 1: Realizar un levantamiento de información del estado actual de la institución educativa departamental Luis Carlos Galán.

- Identificar de los activos: Para identificar los activos que se encuentran en la institución, se solicitara a secretaria el inventario, se realizaran entrevistas, lista de chequeo y observación directa de la sede principal Luis Carlos Galán.

- Determinar de los dominios de información: Se realizaran valoraciones a los activos, determinando la confidencialidad, integridad y disponibilidad de estos.

6.3.2 Objetivo 2: Elaborar un plan de auditoría de acuerdo a la información recolectada.

- Evaluar los diferentes aspectos que involucran el buen funcionamiento de la institución, como son: infraestructura, entorno, equipos, entre otros.

- Preparar y realizar con eficiencia las responsabilidades asignadas.

- Recoger y analizar datos para obtener conclusiones relativas al SGI auditado en la institución.

6.3.3 Objetivo 3: Realizar las respectivas recomendaciones de acuerdo a los resultados obtenidos en la auditoria.

- Realizar entrevistas a funcionarios, contratistas y otras personas que puedan afectar el proceso en la institución.

- Aprobar las estructuras administrativas y dictar los correspondientes manuales de procedimiento.

- Aplicar las normas recomendadas durante la auditoria.

6.3.4 Objetivo 4: Realizar un informe de auditoría para la institución educativa.

- Exponer los hechos, analizar las causas y recomendar acciones correctoras.

- Registrar todas las actividades descritas en el plan de auditoría.

6.4 POBLACIÓN DE INVESTIGACIÓN

El área de investigación se llevará a cabo en la instalación principal de la institución. El cual se encuentra ubicado en la Inspección de Terán, Municipio de Yacopí-Cundinamarca.

6.5 ALCANCE DE LA INVESTIGACIÓN

Al momento de realizar la auditoria en la institución, empezaremos por el levantamiento de la información, la cual será realizada por medio de una encuesta, que permitirá establecer el nivel riesgo en la que está la institución.
Una vez determinados los riesgos, se procede a informar a la institución, de los resultados obtenidos durante el proceso de observación, entrevistas y encuestas.

Luego se procede a implementar herramienta Metodología Margerit la cual lograra mitigar los riesgos al igual se realiza un análisis de vulnerabilidades de las plataformas tecnológicas en las que se realiza los procedimientos institucionales. Para después entregar un informe final con la recomendación a implementar en la seguridad informática de la institución.

El estudio se enfocará en la oficina de la secretaria, coordinación, rectoría y sala de profesores de la sede principal de la institución.

Estas oficinas cuentan con 15 empleados, entre los cuales se tienen: Rector, un Coordinador, una Secretaria, una persona de aseo y once docentes. Igualmente se cuenta con cinco oficinas, 30 equipos de cómputo, 4 impresoras multifuncionales en red, internet banda ancha, un cuarto técnico con equipos de comunicación como: *Switch, Router y Patch panel*.

7. INFORME TÉCNICO

A continuación se presentan las etapas para la ejecución del análisis de riesgos se adopta el ciclo de mejora continua PHVA[29] como lo recomienda la norma ISO/IEC 27001.

Etapa 1:

Donde se realiza el reconocimiento de la infraestructura física y tecnológica, como también la recolección de información y documentación para el desarrollo del proyecto:

- Información contextual de la Institución.

- Manuales de configuración el cual estará elaborado por personal del área en cuanto a servicios, servidores y dispositivos en red.

- Estudios o contrataciones relacionados con seguridad de la información.

- Manuales diseñados para los usuarios, manuales de operación de sistema de información propios o de terceros.

- Procesos y procedimientos definidos del personal de soporte técnico o de atención a usuarios para la solución de incidencias

Etapa 2:

Después de comprender la estructura organizacional y su forma de operar, se procede a clasificar los activos por criticidad, definiendo planes a realizar y obteniendo datos donde identifique el estado de seguridad a nivel de hardware y software de los equipos, servicios, información de las instalaciones físicas procesos y procedimientos.

- Identificar los sitios de los equipos de comunicación donde se encuentran, seguridad perimetral, almacenamiento y procesamiento de datos; esto debido al recolectamiento de vivencias de las condiciones actuales.

- Los activos se clasifican para determinar cuáles son los más críticos que puedan detener el funcionamiento de la institución en caso de falla.

[29] SECURITY JEIFER. ¿Qué es ciclo PHVA?. Enero 09 de 2010. Blog de seguridad informática. [on líne], [consultado el 2 de septiembre de 2017]. Disponible en internet: http://securityjeifer. wordpress.com/tag/phva/

- Se solicitan cuentas de prueba, accesos a servidores y equipos de comunicación, como *firewall, switches y routers*, con el fin de tomar evidencias de los procesos y la forma de configuración de cada dispositivo y/o sistema operativo.

Etapa 3:

Ya obtenida la información y el acceso a los servidores, equipos y servicios, y conociendo el direccionamiento e infraestructura tecnológica, se procede a realizar pruebas, basados en herramientas de escaneo y análisis para poder detectar posibles vulnerabilidades, como también determinando el estado actual de la seguridad en la infraestructura de red e información general.

- Para la realización de pruebas en el contexto del proyecto, se utilizan herramientas y diferentes entornos, donde estas herramientas son de tipo *Ethical Hacking* con herramientas en línea y versiones de prueba.

- Se identifican puertos, protocolos y servicios para determinar el estado actual de los puertos disponibles, abiertos y cerrados. Llegando así a realizar el análisis de riesgos informáticos sobre los servicios de red y aplicaciones por su criticidad.

- Después de haber realizado un análisis de riesgos, se procede a realizar un escaneo de vulnerabilidades previamente seleccionadas, donde se evaluaron las diferentes formas de ataques, como de acceso de fuerza bruta sobre aplicativos web, tipo de codificación y/o cifrado de contraseñas y cifrado de las mismas, como también pruebas de acceso entre subredes y segmentos con tal de evadir los sistemas de protección física y lógica, como *Vlansy switches*, sistema *VPN* y políticas de restricción en zonas configuradas con *firewall*; dentro de las diferentes pruebas que se realizaron, se realizó la prueba de escalamiento de privilegios y acceso remoto.

- Con la información obtenida, se procede a realizar un análisis y clasificación de activos que se encuentran en riesgo, determinando controles y salvaguardas, de tal manera que minimice el impacto de materialización de amenaza detectada.

7.1 ACTIVOS DE INFORMACIÓN

Actualmente la Institución Educativa Departamental Luis Carlos Galán del Municipio de Yacopí Cundinamarca, tiene los siguientes activos de información e infraestructura tecnológica:

7.1.1 Servidores y Equipos de Intercambio de Datos

- La institución posee un (1) servidor.
- Encargado del control de acceso en el salón de sistema.
- Sistema Operativo Windows Server 2008, marca hp.
- Dos (2) zonas de acceso inalámbrico.
- Red de internet.
- Un *swithes* de red.
- Dos *routers*.

7.1.2 Sistemas de Seguridad, Prevención y Control de Acceso

- Sensores de movimiento y alarmas de seguridad.
- Ubicadas en secretaria y salón de sistemas, administrada por la misma institución.
- Cámaras de seguridad IP.
- Ubicadas en secretaria y salón de sistemas, administrada por la misma institución.
- Sistema de aire acondicionado.
- Extintores de diferentes tipos según la ubicación del extintor, entorno, equipos y elementos de cada sitio.

7.1.3 Equipos de Cómputo

La sede principal dispone de treinta y tres (33) equipos de cómputo, distribuidos de la siguiente manera, veintidós (22) equipos de cómputo en la sala de sistemas y dos (2) en laboratorio, sumando 24 equipos de uso estudiantil. Nueve (9) equipos de cómputo para uso administrativo y docente.

7.2 ETHICAL HACKING. ANÁLISIS DE VULNERABILIDADES

El informe técnico ayudará a identificar, por medio de algunas de las pruebas de análisis y resultados obtenidos con las herramientas utilizadas y teniendo presente a nivel de guía, la metodología *MAGERIT v.3* para el análisis y gestión de los riesgos encontrados, determinando así las posibles fallas, amenazas y vulnerabilidades que se puedan estar presentando en la Institución Educativa Departamental Luis Carlos Galán, al estar afectando de forma directa o indirecta la seguridad de la información que se administra o manipula el personal administrativo y docente.

El objetivo de este proyecto es hacer énfasis en los servicios que actualmente se prestan en la institución, siendo estos fundamentales en el funcionamiento diario

institucional, donde se pueden presentar fallas, daños o alteraciones a dichos servicios por la ausencia de procedimientos, políticas, planes y mecanismos que garanticen la confiabilidad, confidencialidad y disponibilidad de la información.

7.2.1 Evaluación de Vulnerabilidades

Cuadro 1: Evaluación de vulnerabilidades

Evaluación de vulnerabilidades 1	
Prueba efectuada	Se procede a identificar y a enumerar los puertos, servicios y protocolos, como lo son la identificación del direccionamiento público y privado IPv4, de acuerdo a los segmentos 190.XX.XXX.XXX y 168.XX.XX.XXX. Dicha prueba se realizó utilizando herramientas como *Nmpa, ping* y *zenmap*.
Fecha de duración	Marzo 1 de 2016 – 2:00 pm a 5:00 pm (Direcciones públicas) Marzo 4 de 2016 – 2:00 pm a 5:00 pm (Direcciones privadas)
Encargado de prueba	José Edwin González Retamozo Wilson Vaca
Conclusiones	Se pudo establecer que la protección de los *firewalls* se encuentra bastante restrictiva a nivel del direccionamiento público obedeciendo a las políticas establecidas de restricción de servicios y protocolos en el *Firewall*. En el direccionamiento privado se detectaron puertos abiertos, debido a que no se han establecido políticas restrictivas, ya que se obtuvo información de los servicios y puertos abiertos.

Evaluación de vulnerabilidades 2	
Prueba efectuada	Una vez identificados los puertos y servicios específicos de los activos de la institución, se procede a ejecutar pruebas con herramientas que permitieron encontrar y analizar las vulnerabilidades, entre estas tenemos: *Nessus* y *Nikto*. Identificando fallos a nivel de sistemas operativos, aplicativos o servicios.

Evaluación de vulnerabilidades (continuación)

Activo de información	Servidores de sitios web críticos, por direcciones públicas, Sistemas de Servidores de Información logística (GLPI), Servidores SIMAT y Servidor SIGES.
Fecha de duración	Marzo 8 de 2016 (2:00 pm) hasta Marzo 11 de 2016 (5:00 pm)
Encargado de prueba	José Edwin González Retamozo Wilson Vaca
Conclusiones	De acuerdo a los resultados obtenidos provistos por las herramientas de detección de vulnerabilidades, se establecieron vulnerabilidades tipo ransomware, como también en niveles de versiones obsoletas en sistemas operativos al igual que las versiones que tienen alto riesgo de amenazas y vulneración en servidores web.
Evaluación de vulnerabilidades 3	
Prueba efectuada	Se efectuaron pruebas al SIGES, determinando el desarrollo de módulos web, a nivel de scripts, variables y chequeo de código de bajo rendimiento.
Activo de información	Sistema de Información para la Gestión Escolar SIGES, se reconocieron los módulos internos y externos, determinando la evaluación en línea, generación de boletines y libros de notas de años anteriores.
Fecha de duración	Marzo 15 al 16 en horas de la tarde.
Encargado de prueba	Mauricio Torres Bautista José Edwin González R.
Conclusiones	Se pudo establecer que dentro de una prueba interna el rendimiento de algunos módulos se ven saturados frente a un script provocando denegaciones de un servicio después de un corto periodo de tiempo.

Evaluación de vulnerabilidades (continuación)

Evaluación de vulnerabilidades 4	
Prueba efectuada	Se efectuaron pruebas al SIMAT, determinando el desarrollo de módulos web, a nivel de scripts, variables y chequeo de código de bajo rendimiento.
Activo de información	Sistema Integrado de Matriculas SIMAT, se reconocieron los módulos internos y externos, determinando los alumnos matriculados en cada sede, la matrícula de un estudiante y el retiro de éste.
Fecha de duración	Marzo 17 al 18 en horas de la tarde.
Encargado de prueba	Mauricio Torres Bautista José Edwin González R.
Conclusiones	Se pudo establecer que dentro de una prueba interna el rendimiento de algunos módulos se ven saturados frente a un script provocando denegaciones de un servicio después de un corto periodo de tiempo

Evaluación de vulnerabilidades 5	
Prueba efectuada	Se realizaron pruebas de verificación de contraseñas a los sistemas web de acceso a SIGES y SIMAT.
Activo de información	Servidores web de SIGES y SIMAR.
Fecha de duración	Marzo 19 en horas de la mañana
Encargado de prueba	José Edwin González Retamozo Wilson Vaca
Conclusiones	Con la utilización de la herramienta de John The Ripper, se pudo establecer que las contraseñas no son seguras y que muchas son fáciles de descifrar en los sistemas web SIGES y SIMAT .

Evaluación de vulnerabilidades (continuación)

Evaluación de vulnerabilidades 6	
Prueba efectuada	De acuerdo a las vulnerabilidades presentadas, se realizaron pruebas de penetración, utilizando las herramientas de tipo httpprint comparando las firmas de versiones del web server objeto de análisis con las listas de explotación y fallas a nivel de configuración o codificación.
Activo de información	Se realizará pruebas de vulnerabilidades a los servidores y aplicativos web de SIGES y SIMAT que enlacen a los módulos o sistemas de información sensibles, los cuales fueron virtual izados por Virtual Box como ambiente de laboratorio de pruebas.
Fecha de duración	Marzo 21 en hora de la mañana
Encargado de prueba	José Edwin González Retamozo Wilson Vaca
Conclusiones	Se demostró que existen fallas de seguridad, como fueron las malas prácticas para la asignación de passwords.

Fuente: autor

7.3 RESUMEN INFORMATIVO Y FUNCIONAL DE LOS SISTEMAS DE INFORMACIÓN SENSIBLES

A continuación se presenta un resumen informático y funcional de los sistemas de información sensibles que presenta la institución:

7.3.1 GLPI. (Gestionnaire Libre de Parc Informatique). Es un sistema de seguimiento de incidencias de hardware y software, permitiendo el registro y administración de inventarios de los recursos informáticos. Este software funciona internamente, siendo este una aplicación web bajo código abierto en PHP.

7.3.2 Sistema Integrado de Matriculas SIMAT. El sistema integrado de matrícula SIMAT es una herramienta que permite organizar y controlar el proceso de matrícula en todas sus etapas, así como tener una fuente de información confiable y disponible para la toma de decisiones.

SIMAT es un sistema de gestión de la matrícula de los estudiantes de instituciones oficiales y no oficiales que facilita la inscripción de alumnos nuevos, el registro y la actualización de los datos existentes de un alumno, la consulta de alumnos por Institución, el traslado del alumno a otra Institución, así como la obtención de informes como apoyo para la toma de decisiones.

Figura 3. Ministerio de Educación Nacional

Fuente: (MINISTERIO DE EDUCACION NACIONAL, 2017)

7.3.3 Sistema de Información para la Gestión Escolar (Siges). Su propósito es facilitar los procesos académicos y administrativos para lo cual las Secretarias de educación han diseñado un portal en el cual los docentes, directivos y administrativos, se gestiona todo lo relacionado con valoraciones académicas, evaluación, generación de boletines, gestión de matrícula, certificados, entre otros.

Figura 4: Sistema de Información para la Gestión Escolar

Fuente: (SIGES, 2017)

La plataforma debe estar disponible para los procesos de gestión académica, el cual garantice la autenticidad del usuario que ingresa a manejar el aplicativo ya que en este se realizaba todo el proceso académico, siendo importante para los estudiantes matriculados, registrando la admisión y llevando un historial académico del estudiante.

7.4 RESUMEN DEL DIAGNÓSTICO DE LOS SERVICIOS MÁS RELEVANTES

Durante el proceso de pruebas de diagnóstico de vulnerabilidades, se procederá a realizar una prueba de intrusión a uno de los servicios con que cuenta la institución.

En este caso la prueba se realizara al sistema integrado de matrículas SIMAT, al cual se procedió a identificar al servidor la dirección IP, para después determinar el hosting, DNS, propietario, tipo de servidor web, entre otras. Una vez identificadas, se procedió a identificar los puertos que están habilitados.

Durante este proceso se realizaron varios tipos de análisis de riesgos con diferentes herramientas como *nessus, nikton, nmap*, entre otras. Siendo estas herramientas de libre distribución para el hacking ético.

Es importante tener en cuenta que los activos no siempre se miden en los recursos informáticos sino también en los recursos físicos y el ambiental, donde se utilizan técnicas como: la observación directa, la encuesta y el hacking ético; para ello, a continuación se ilustraran algunos ejemplos de revisiones a la seguridad.

7.5 ANÁLISIS Y EVALUACIÓN DE RIESGOS BASADO EN *MAGERIT V3*

Con la metodología *Magerit v3* se implementan tres procesos para el proyecto “Auditoria de Seguridad Informática para La Institución Educativa Departamental Luis Carlos Galán Municipio De Yacopí Cundinamarca”.

7.5.1 Proceso P1: Planificación. Para el desarrollo del proyecto se implementa los siguientes pasos:

7.5.1.1 Actividad A1.1: Estudio de oportunidad. En esta etapa se realiza el estudio diagnóstico del estado de la seguridad de los activos de información y tecnológicos. Como también incentivar a la implementación de un Sistema de Gestión de Seguridad Informática a la institución

7.5.1.2 Actividad A1.2: Definición del alcance y objetivos del proyecto. Una vez aprobada la realización del proyecto “Auditoria de Seguridad Informática para La Institución Educativa Departamental Luis Carlos Galán Municipio De Yacopí Cundinamarca”, se establecen los límites y dominios, definiendo los objetivos a desarrollar del proyecto.

Los objetivos establecidos para el proyecto, se desarrollan revisando y analizando los riesgos llevando a una futura ejecución del sistema de gestión de seguridad de la información de la institución.

7.5.1.3 Actividad A1.3: Planeación del proyecto. De acuerdo con el objetivo del proyecto se realiza el análisis sobre cómo operan los sistemas de información de la institución, evaluando los riesgos inherentes al control definiendo el enfoque a la auditoria que se aplicara y los procedimientos específicos a realizar para el desarrollo exitoso del proyecto.

7.5.1.4 Actividad A1.4: Lanzamiento del proyecto. Con el visto bueno (Ver anexo C) del Rector de iniciar el proceso de análisis de riesgos, se aplica como primera técnica la observación directa y la entrevista, proceso que ayuda a la recolección de información, contando con el apoyo con personal directamente involucrado con los procesos existentes en la institución.

7.5.1.5 Evaluación de vulnerabilidades. Para la recolección de la información se utilizó la metodología *MAGERIT v3*, ya que se ajusta a las necesidades del proyecto.

Para empezar, se debe de caracterizar los activos, el cual consta de tres sub-tareas: Identificación de los activos, dependencia entre los activos y valoración entre los activos. El cual tiene como objetivo reconocer los activos que la componen, definiendo las dependencias que la conforman y así determinando el valor que soporta cada activo.

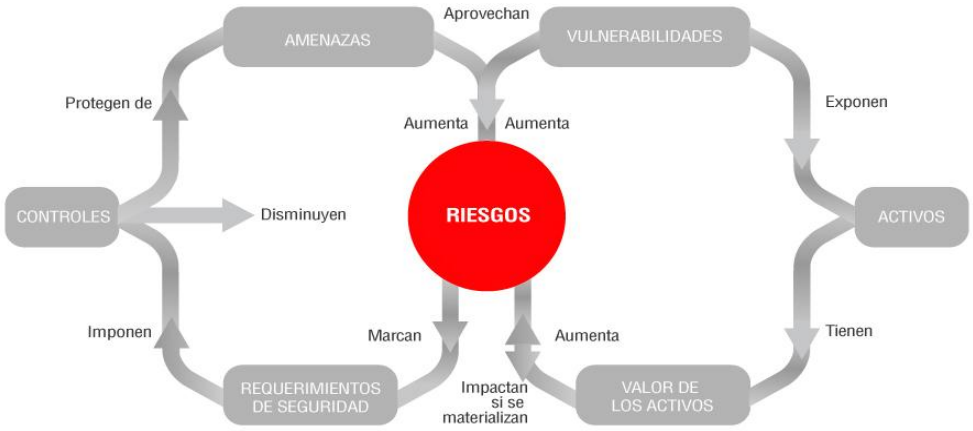
La identificación de los activos, ayudara a determinar las dependencias entre los activos, valorando los activos con precisión, identificar y valorar las amenazas y escoger que salvaguarda utilizar para proteger el sistema.

Entre estos están:

Servicios internos, aplicaciones, equipos, comunicaciones, soportes de información, equipamiento auxiliar, instalaciones y personal.

7.5.2 Proceso P2: Análisis de riesgos.

Figura 5. Análisis de riesgos



Fuente: (SECUREIT, 2017)

La auditoría permite a las organizaciones o instituciones educativas, conocer y valorar los riesgos a los que se ve expuesta, de esta manera es de vital importancia tener en cuenta la normatividad que se lleven a cabo, para que no afecten los activos informáticos.

De aquí la razón de la importancia de ser de *Magerit*, con la correcta aplicabilidad, clasificación y valoración de los activos.

7.5.2.1. Actividad A 2.1 Caracterización y valoración de los activos. A continuación se relacionan las actividades a realizar:

- **Identificación de los activos.** A continuación se relacionan los activos presentes en la institución, identificándolos y clasificándolos, tomando como guía el libro II de la Metodología Magerit v3; catálogo de elementos (Ver anexo A):

Tabla 1. Activos

TIPO	NOMBRE DEL ACTIVO
APLICACIONES INFORMÁTICAS	1. [SI_SIGES] Sistema de Información Académica y de Gestión. 2. [SI_BD] SIMAT Sistema Integrado de Matriculas. 3. [SO] Sistema Operativo. 4. [HER_SW] Herramientas Software. 5. [ANT_VIR] Anti virus
SERVICIOS	6. [SV_DNS] Servidor DNS 7. [SV_DHCP] Servidor DHCP 8. [SV_VoIP] Servidor Telefonía IP 9. [SV_CAM] Servidor Cámaras IP
REDES DE COMUNICACIONES	10. [RO_ISP] *Router* Proveedor de Servicios de Internet.
EQUIPAMIENTO INFORMÁTICO	11. [FW_UTM] *Firewall* / Equipo Unificado contra Amenazas. 12. [PC] Equipos de computo 13. [SW_A] *Switch* Administrable
EQUIPAMIENTO AUXILIAR	14. [CAB_RED] Cableado de Red
PERSONAL	15.[AS_TIC] Asesor Tecnologías de Información y Comunicaciones 16.[TEC_ADMIN_II]Técnico Administrativo Grado II
INSTALACIONES	17. [GAB] Gabinete de red

Fuente: autor

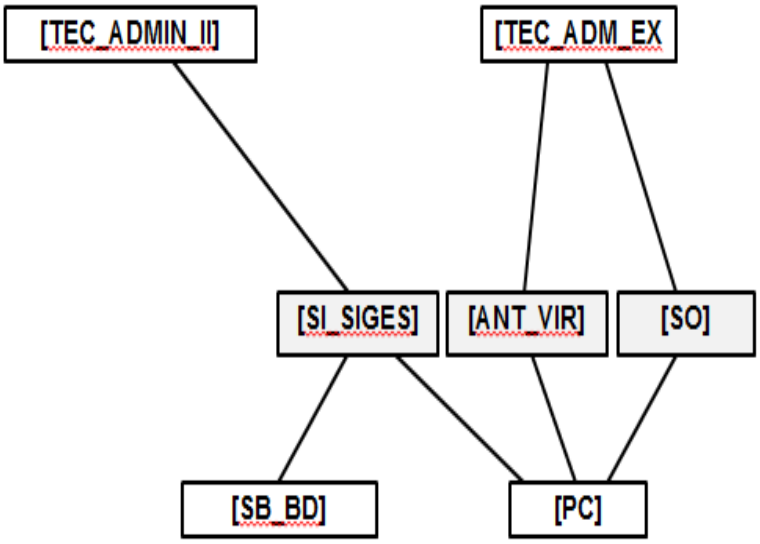
- Dependencias entre activos

Recorrido Top – Down

Dependencia de los activos del tipo APLICACIONES INFORMÁTICAS

- Aplicaciones que los soportan.
- Los equipos que lo hospedan.
- El personal del que depende.

Figura 6. Dependencia de activos tipo aplicación informática

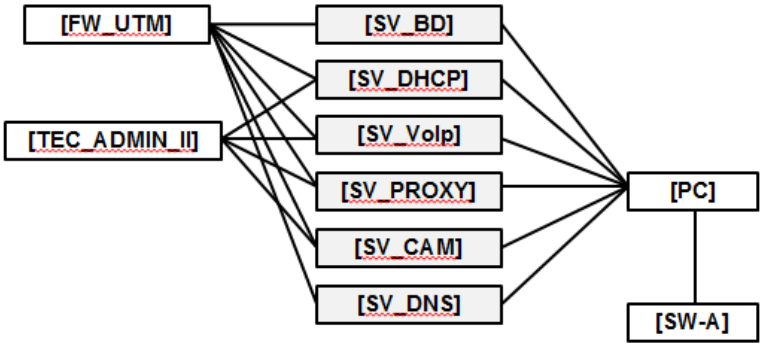


Fuente: autor

Dependencia de los activos del tipo de SERVICIO

- Los equipos que los hospedan
- El personal que tiene acceso

Figura 7. Dependencia de los activos del tipo de servicio

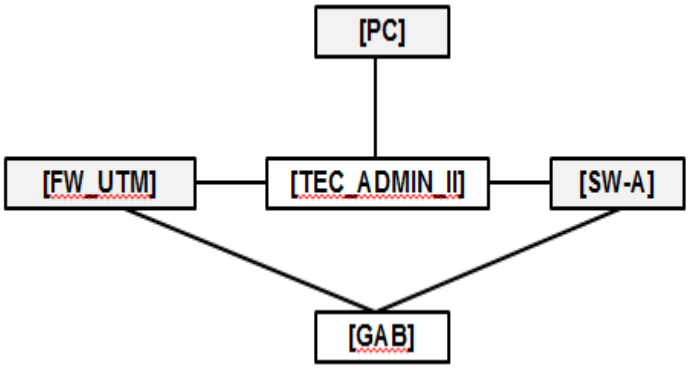


Fuente: autor

Dependencia de los activos del tipo EQUIPAMIENTO INFORMÁTICO

- Los equipos que los hospedan
- El personal que tiene acceso

Figura 8. Dependencia de activos del tipo equipamiento informático

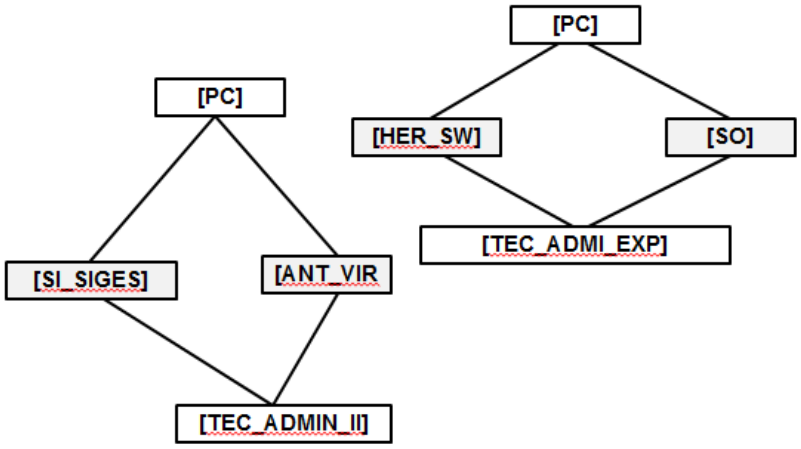


Fuente: autor

Dependencia de los activos del tipo APLICACIONES INFORMÁTICAS

- Los equipos que los hospedan
- El personal que tiene acceso

Figura 9. Dependencia de activos tipo aplicaciones informáticas

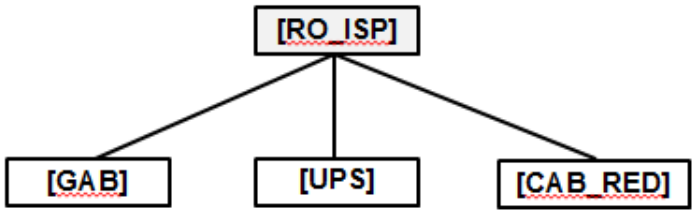


Fuente: autor

Dependencia de los activos del TIPO DE COMUNICACIONES

- Las instalaciones
- El equipamiento auxiliar

Figura 10. Dependencia de los activos del tipo de comunicaciones



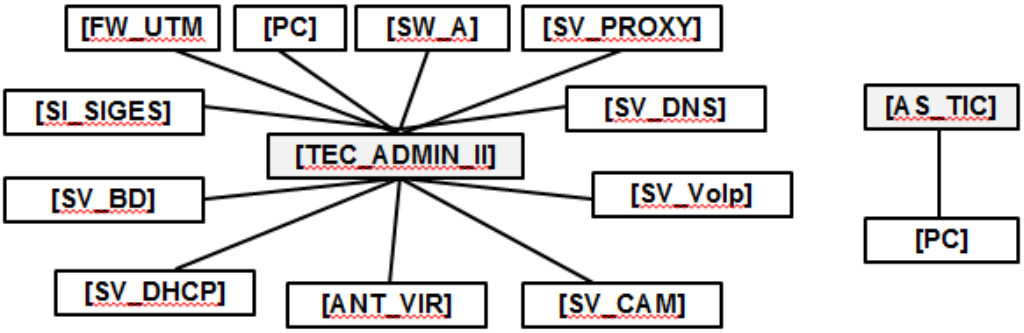
Fuente: autor

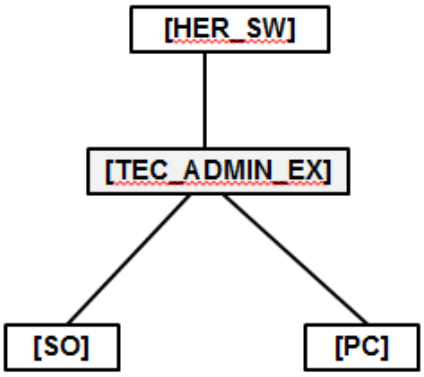
Recorrido Bottom– Up

Los activos que son soportados por el tipo de activos PERSONAL

- Las aplicaciones que manejan
- Los equipos informáticos que gestiona
- Los servicios que gestiona

Figura 11: Los activos que son soportados por el tipo de activo personal.



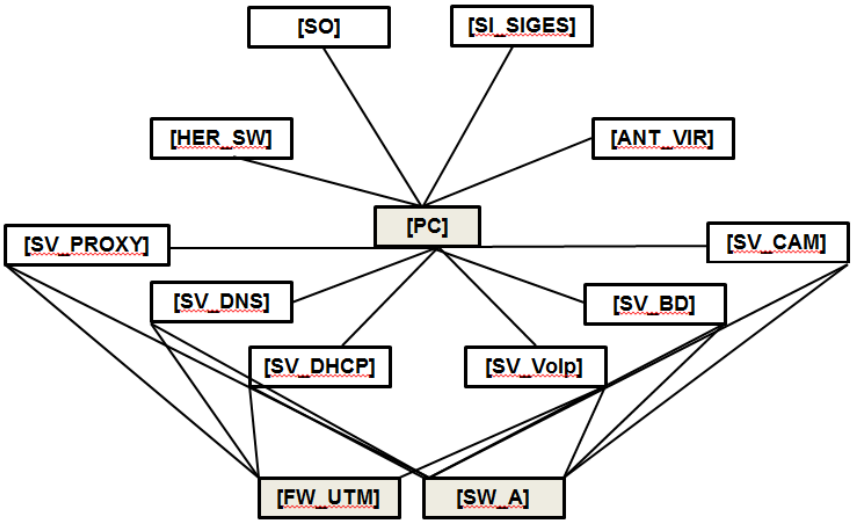


Fuente: autor

Los activos que son soportados por el tipo de activos EQUIPAMIENTO INFORMÁTICO.

- Los servicios habilitan
- Los datos que hospeda

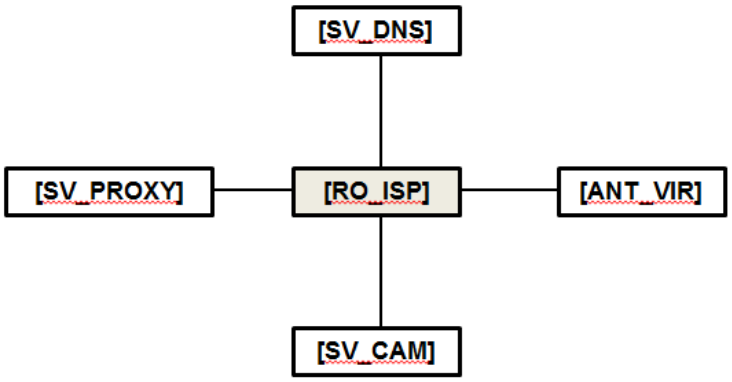
Figura 12. Los activos que soportan por el tipo de activos equipamiento informático.



Fuente: autor

Los activos que son soportados por el tipo de activos REDES DE COMUNICACIONES.

- Las aplicaciones que habilita
- Los servicios que habilita

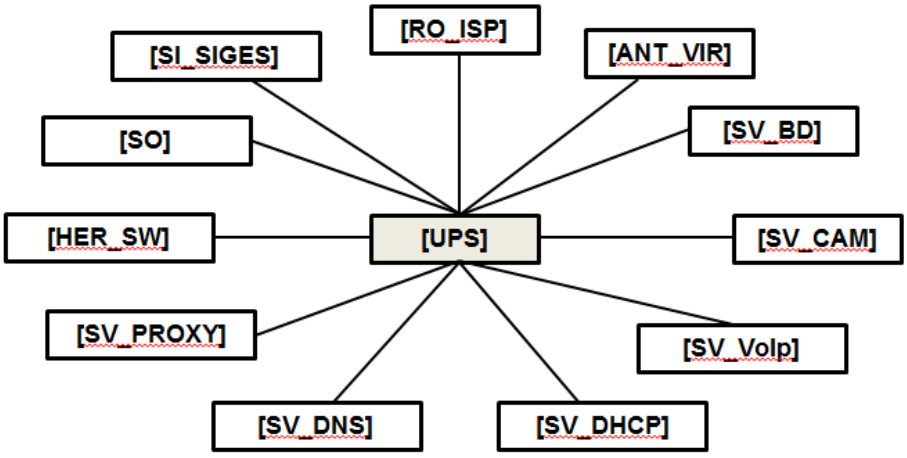


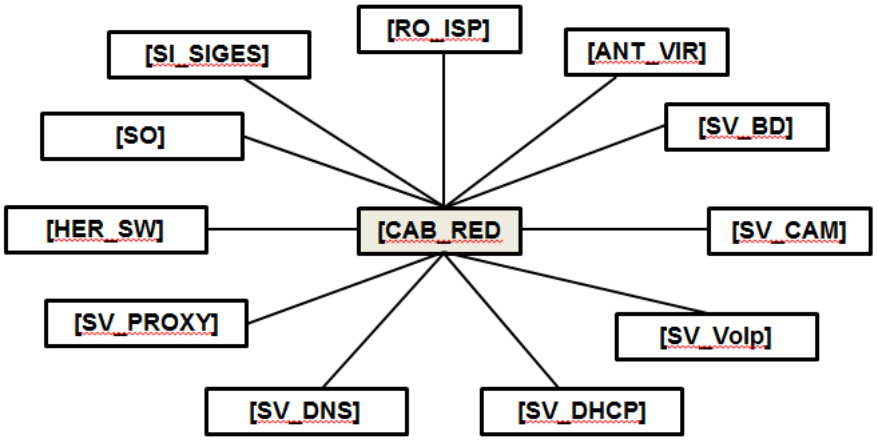
Fuente: autor

Los activos que son soportados por el tipo de activos EQUIPAMIENTO AUXILIAR.

- Las redes de comunicación
- Las aplicaciones que habilita
- Los servicios que habilita

Figura 13: Los activos que son soportados por el tipo de activos equipamiento auxiliar.





Fuente: autor

Los activos que son soportados por el tipo de activos INSTALACIONES.

- Los equipos informáticos que acoge.

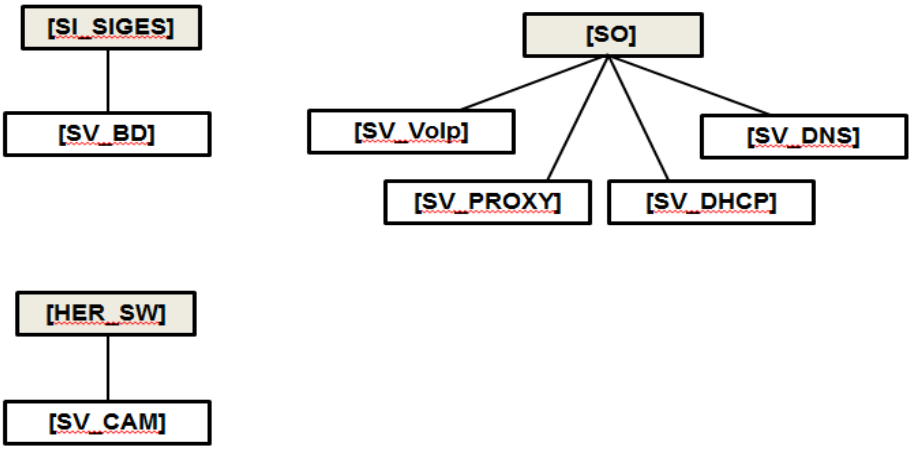
Figura 14. Los activos que son soportados por el tipo de activos instalaciones.

Fuente: autor

Los activos que son soportados por el tipo de activos APLICACIONES

- Los servicios que habilita

Figura 15. Los activos que son soportados por el tipo de activos aplicaciones.



Fuente: autor

- Valoración de los activos. Para realizar la valoración de los activos, se debe tener en cuenta las siguientes consideraciones:

- Dimensiones en la que el activo es relevante.
- Estimación de la valoración en cada dimensión.

Cuadro 2: Criterios de evaluación

Nivel	Criterio
3	Alto
2	Medio
1	Bajo
0	Depreciable

Fuente: autor

Dimensiones

- [D] Disponibilidad
- [I] Integridad de los datos
- [C] Confidencialidad de los datos
- [A] Autenticidad de los usuarios y de la información
- [T] Trazabilidad del servicio y de los datos

Valoración de Activos Tipo: Aplicaciones

Tabla 2. Valoración de activos tipo: Aplicaciones

Activo	Dimensiones de seguridad				
	[D]	[I]	[C]	[A]	[T]
1.[SI_SIGES] Sistema De Información Para La Gestión Escolar (Siges).	[2]	[2]	[2]	[1]	[2]
2. [SI_BD] SIMAT Sistema integrado de matrículas (SIMAT)	[2]	[2]	[2]	[2]	[3]
3. [SO] Sistema Operativo.	[1]	[2]	[3]	[2]	[2]
4.[HER_SW] Herramientas Software	[3]	[2]			
5.[ANT_VIR] Antivirus	[2]				

Fuente: autor

a) **[4.pi1]** probablemente afecte a un grupo de individuos
[5.lro] probablemente sea causa de incumplimiento de una ley o regulación
[1.po] pudiera causar protestas puntuales.
[10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
[1.lg] Pudiera causar una pérdida menor de la confianza dentro de la Organización.

b) **[4.pi1]** probablemente afecte al grupo de administración.
[5.lro] probablemente sea causa de incumplimiento de una ley o regulación
[1.po] pudiera causar protestas puntuales.
[10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
[1.lg] Pudiera causar una pérdida menor de la confianza dentro de la Organización
[6.pi2] probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.
[7.lro] probablemente cause un incumplimiento grave de una ley o regulación.
[3.si] probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente.
[3.da] Probablemente cause la interrupción de actividades propias de la Organización.
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.

c) **[6.pi2]** probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
[7.lro] probablemente cause un incumplimiento grave de una ley o regulación
[3.si] probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.

d) **[7.si]** probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
[7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones

Valoración de Activos Tipo: Servicios

Tabla 3. Valoración de Activos Tipo Servicios

Activo	Dimensiones de seguridad				
	[D]	[I]	[C]	[A]	[T]
5.[SV_PROXY] Servidor Proxy.	[3]	[2]	[2]		
6. [SV_DHCP] Servidor DHCP	[3]	[2]			
7. [SV_VoIP] Servidor Telefonía IP	[1]	[1]			
8. [SV_CAM] Servidor Cámaras IP	[1]				

Fuente: autor

e) **[6.pi1]** probablemente afecte gravemente a un grupo de individuos.
[9.si] probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios.
[9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones.
[6.po] probablemente cause manifestaciones, o presiones significativas
[3.adm] probablemente impediría la operación efectiva de una parte de la Organización.

f) **[1.pi1]** pudiera causar molestias a un individuo
[3.si] probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
[9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
[6.po] probablemente cause manifestaciones, o presiones significativas
[3.adm] probablemente impediría la operación efectiva de una parte de la Organización

g) **[6.pi1]** probablemente afecte gravemente a un grupo de individuos
[9.si] probablemente sea causa de un serio incidente de seguridad o dificulté la investigación de incidentes serios
[9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
[6.po] probablemente cause manifestaciones, o presiones significativas
[3.adm] probablemente impediría la operación efectiva de una parte de la Organización
[9.lg.a] Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones.

h) **[4.pi1]** probablemente afecte a un grupo de individuos
[3.lro] probablemente sea causa de incumplimiento leve o técnico de una ley o regulación.
[9.si] probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[3.adm] probablemente impediría la operación efectiva de una parte de la Organización
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización
[6.lbl] Difusión limitada

Valoración de Activos Tipo: Redes de Comunicaciones

Tabla 4. Valoración de Activos Tipo: Redes de Comunicaciones

Activo	Dimensiones de seguridad				
	[D]	[I]	[C]	[A]	[T]
9. [RO_ISP] Router Proveedor de Servicios de Internet.	[3]	[2]			

Fuente: autor

i) **[5.pi2]** probablemente quebrante seriamente leyes o regulaciones
[9.lro] probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación.
[10.si] probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios.
[9.cei.e] constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros.
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística.
[5.lg.b] Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público.

Valoración de Activos Tipo: Equipamiento Informático

Tabla 5. Valoración de Activos Tipo: Equipamiento Informático

Activo	Dimensiones de seguridad				
	[D]	[I]	[C]	[A]	[T]
10.[FW_UTM] *Firewall* / Equipo Unificado contra Amenazas.	[3]	[2]	[3]	[3]	[2]
11.[PC] Equipos de cómputo	[2]	[2]	[3]	[2]	
12.[SW_A] *Switch* Administrable	[2]	[2]	[3]	[2]	

Fuente: autor

j) **[6.pi2]** probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.
[7.lro] probablemente cause un incumplimiento grave de una ley o regulación

[10.si] probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios.
[9.cei.e] constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros.
[9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones.
[6.po] probablemente cause manifestaciones, o presiones significativas
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.
[2.lg] Probablemente cause una pérdida menor de la confianza dentro de la Organización.

k) **[5.pi1]** probablemente afecte gravemente a un individuo
[3.lro] probablemente sea causa de incumplimiento leve o técnico de una ley o regulación.
[7.si] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
[7.cei.d] proporciona ganancias o ventajas desmedidas a individuos u organizaciones
[5.da] Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
[1.po] pudiera causar protestas puntuales
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización.

l) **[5.pi1]** probablemente afecte gravemente a un individuo
[3.lro] probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
[7.si] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
[7.cei.d] proporciona ganancias o ventajas desmedidas a individuos u organizaciones
[7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
[6.po] probablemente cause manifestaciones, o presiones significativas
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[5.lg.b] Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público

Valoración de Activos Tipo: Equipamiento Auxiliar

Tabla 6: Valoración de Activos Tipo: Equipamiento Auxiliar

Activo	Dimensiones de seguridad				
	[D]	[I]	[C]	[A]	[T]
13. [CABREAD] Cableado de Red.	[2]	[2]			[2]
14. [FA_UPS] Sistema de Alimentación Ininterrumpida.	[2]				

Fuente: autor

ll) **[4.pi1]** probablemente afecte a un grupo de individuos
[3.si] probablemente sea causa de una disminución en la seguridad o dificulte la investigación de un incidente
[7.cei.d] proporciona ganancias o ventajas desmedidas a individuos u organizaciones
[7.da] probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
[6.po] probablemente cause manifestaciones, o presiones significativas
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.adm] probablemente impediría la operación efectiva de la Organización

m) **[4.pi1]** probablemente afecte a un grupo de individuos
[3.si] probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
[3.adm] probablemente impediría la operación efectiva de una parte de la Organización
[6.po] probablemente cause manifestaciones, o presiones significativas

Valoración de Activos Tipo: Personal

Tabla 7. Valoración de Activos Tipo: Personal

Activo	Dimensiones de seguridad				
	[D]	[I]	[C]	[A]	[T]
15. [AS_TIC] Asesor Tecnologías de Información y Comunicaciones	[2]		[3]		[1]
16. [TEC_ADMIN_II] Técnico Administrativo	[1]	[2]	[2]	[2]	[1]

Fuente: autor

n) **[6.pi1]** probablemente afecte gravemente a un grupo de individuos
[7.si] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
[3.cei.d] facilita ventajas desproporcionadas a individuos u organizaciones
[7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
[5.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.
[6.po] probablemente cause manifestaciones, o presiones significativas
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.
[5.adm] probablemente impediría la operación efectiva de más de una parte de la Organización.
[7.lg.b] Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general.

o) **[6.pi1]** probablemente afecte gravemente a un grupo de individuos.
[9.lro] probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación.
[9.si] probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios.
[9.cei.b] de muy elevado valor comercial
[9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones.
[3.po] causa de protestas puntuales
[10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
[7.adm] probablemente impediría la operación efectiva de la Organización
[9.lg.b] Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
[4.crm] Dificulte la investigación o facilite la comisión de delitos

Valoración de Activos Tipo: Instalaciones

Tabla 8. Valoración de Activos Tipo: Instalaciones

Activo	Dimensiones de seguridad				
	[D]	[I]	[C]	[A]	[T]
17. [GAB] Gabinete de Red.	[1]	[1]			

Fuente: autor

p) **[1.lro]** pudiera causar el incumplimiento leve o técnico de una ley o regulación.
[1.si] pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

7.5.2.2 Caracterización de las amenazas. Para la caracterización, se utiliza la herramienta PILAR estandarizada por *MAGERIT v3*; se clasifican las amenazas en cuatro grupos:

- [N] Desastres naturales.
- [I] De origen natural.
- [E] Errores y fallos no intencionados.
- [A] Ataque intencionado.

El objetivo es identificar el riesgo al cual se enfrenta el sistema, lo que pueda pasar, consecuencias y como de probable es que pase.

Frecuencia de amenazas

Tabla 9. Frecuencia de amenazas

VALOR	VULNERABILIDAD		CRITERIO
4	Muy frecuente	MF	1 vez al día
3	Frecuente	F	1 vez cada semana
2	Normal	FN	1 vez al año
1	Poco frecuente	PF	Cada varios años

Fuente: (*MAGERIT V 3*, 2010)

Tabla 10. Degradación de las amenazas

VALOR		CRITERIO
100%	MA	Degradación muy alta del activo
80%	A	Degradación alta del activo
50%	M	Degradación mediana del activo
10%	B	Degradación baja del activo
1%	MB	Degradación muy baja del activo

Fuente: (*MAGERIT V 3*, 2010)

Identificación y Valoración de Amenazas Tipo: Aplicaciones Informáticas

Tabla 11. Valoración de Amenazas Tipo: Aplicaciones Informáticas

Activo/Amenaza	Frecuencia	Dimensión de seguridad				
		D	I	C	A	T
[E.1] Errores de los usuarios	F	MA	A			
[E.2] errores del administrador	FN	A				
[E.4] Errores de Configuración	FN	M				
[E.14] Escapes de información	PF			A		
[E.18] Destrucción de información	PF	A		A		
[A.11] Acceso no autorizado	FN	MA				
[A.15] Modificación de la información	PF		MA			

Fuente: autor

Justificación de Amenazas – Aplicaciones informáticas

[E.1] Errores de los usuarios: Se presenta esta amenaza debido a que el personal no es capacitado y no es consciente del valor de los activos que manejan, teniendo un impacto en la disponibilidad muy alto.

[E.2] Errores del administrador: En la dimensión disponibilidad se le da un valor de Alto, debido a que tiene el acceso a diferentes aplicaciones, viéndose seriamente afectados, aunque la probabilidad de ocurrencia sea poco frecuente.

[E.4] Errores de configuración: Se valoró como mediana, ya que la configuración que realicen los usuarios podrían presentar suplantaciones, y cierre de notas, robo de información, afectando la institución educativa departamental Luis Carlos Galán.

[E.14] Escapes de información: se valora la dimensión como Alta, ya que si hay escape de información, ésta podría ser modificada o usada para beneficios propios, perdiendo confidencialidad y confianza institucional.

[E.18] Destrucción de información: Se consideró como una amenaza alta en disponibilidad y confidencialidad, ya que donde puedan versen afectadas los activos de información.

[A.11] Acceso no autorizado: Esta dimensión es calificada muy alta, debido a la falta de capacitación del personal, pudiendo desencadenar varias amenazas como las anteriores.

[E.15] Modificación de la información: En la integridad de los datos, se calificó muy alta, debido a que la afectaría directamente. Provocando caos informático y arrojando datos erróneos a la hora de las consultas.

Identificación y valoración de amenazas: Servicios.

Tabla 12. Identificación y valoración de amenazas: Servicios.

Activo/Amenaza	Frecuencia	Dimensión de seguridad				
		D	I	C	A	T
[E.20] Vulnerabilidades de los programas	FN	MA				
[A.5] Suplantación de la identidad del usuario	F			A	A	
[A.8] Difusión de software dañino	FN	A				
[A.24] Denegación de servicios.	PF	A		A		

Fuente: autor

Justificación de amenazas: Servicios

[E.20] Vulnerabilidades de los programas: Se consideró la probabilidad de FN (Normal) afectando la disponibilidad directamente. En caso de sufrir un ataque la amenaza se considera una suspensión de los servicios en un nivel muy alto.

[A.5] Suplantación de la identidad del usuario: Se consideró una de las mayores amenazas, ya que el personal de la institución no posee capacitación y no tiene implementado un plan de normatividad para el uso de los servicios.

[A.8] Difusión de software dañino: Dentro del nivel de frecuencia se considera normal y la dimensión de probabilidad se considera de alto grado. Debido a que los equipos en su mayoría se encuentran destinados a los estudiantes de la institución y estos no tienen concientización del uso de software licenciado.

[A.24] Denegación de servicios: se consideró poco frecuente su frecuencia de ocurrencia, pero en el nivel de degradación se considera alta, ya que se pueden presentar errores de programación, provocando el bloqueo de acceso a usuarios autorizados al sistema.

Identificación y valoración de amenazas: redes de comunicaciones.

Tabla 13. Identificación y valoración de amenazas: redes de comunicaciones

Activo/Amenaza	Frecuencia	Dimensión de seguridad				
		D	I	C	A	T
[N.*] Desastres naturales	PF	MA				MA
[I.5] Avería de origen físico y lógico	PN	MA				
[I.8] Fallo de servicio de comunicaciones	PF	A				
[E.2] Errores del administrador	PF	A		A		
[E.4] manipulación de configuración.	PF			A	A	

Fuente: autor

Justificación de amenazas – redes de comunicaciones

[N.*] Desastres naturales: Se pueden llegar a presentar, debido a las condiciones geográficas rurales donde se encuentra, el cual tendría un detrimento muy alto, ya que podría causar una paralización de todas las actividades.

[I.5] Avería de origen físico y lógico: Dentro del nivel de frecuencia se considera normal, ya que por las condiciones climáticas sea amenazada, pero en la dimensión la disponibilidad se encuentra en un nivel muy alto, ya que las condiciones donde se encuentran no son las adecuadas físicamente para su protección.

[I.8] Fallo de servicio de comunicaciones: El nivel de frecuencia fue calificado como poco frecuente, pero en la dimensión de seguridad fue catalogado como alto, ya que en el momento en que falle el servicio se ve afectado por varia horas.

[E.2] Errores del administrador: La parte del administrador fue calificado como poco frecuente, pero en la dimensión de seguridad está en un nivel de degradación alto, ya que este servicio no es propio de la administración si no de la empresa que presta el servicio.

[E.4] manipulación de configuración: El nivel de frecuencia es calificado poco frecuente, pero en las dimensiones de confidencialidad y autenticidad son consideradas de alto riesgo, ya que la configuración la administra la empresa que presta el servicio.

Identificación y valoración de amenazas: Equipamiento informático

Tabla 14. Identificación y valoración de amenazas: Equipamiento informático.

Activo/Amenaza	Frecuencia	Dimensión de seguridad				
		D	I	C	A	T
[N.1] Fuego	PF	MA	MA	MA	MA	MA
[I.2] Daños por agua	PF	MA	MA	MA	MA	MA
[I.5] Avería de origen físico y lógico.	PF	A				
[E.23] Errores de mantenimiento / actualización de equipos (Hardware).	FN	A				
[A.11] Acceso no autorizado	FN			A		
[A.23] Manipulación de los equipos.	FN			A		

Fuente: autor

Justificación de amenazas – Equipamiento informático.

[N.1] Fuego: En todas las dimensiones es considerado de muy alto impacto, ya que los equipos informáticos no cuentan con protección contra ésta amenaza y no existe unas políticas establecida ante ésta emergencia.

[I.2] Daños por agua: Es considerado como muy alta en degradación y poco frecuente, debido a que los equipos informáticos anteriormente fueron dañados por un vendaval que ocurrió en la zona, el cual daño el techo de la sala. Provocando el fuera de servicio de éste.

[I.5] Avería de origen físico y lógico: La degradación se consideró alta, ya que el equipamiento informático se encuentra expuesto a la vulnerabilidad de insectos como las avispas que crean sus nidos dentro de estos equipos, como también son sometidas a largas jornadas de uso, los cuales en ocasiones el mal uso ha provocado daños físicos y lógicos.

[E.23] Errores de mantenimiento / actualización de equipos (Hardware): Es valorada con un alto impacto, debido a que los equipos de cómputo que son de aula, son utilizados para prácticas de laboratorio del SENA y no se cuenta con políticas de mantenimiento.

[A.11] Acceso no autorizado: En esta dimensión ésta valorada en un nivel alto, ya que no se encuentran normas de seguridad implementas y la sala de cómputo se encuentra expuesta al acceso de cualquier persona, debido al Kiosco Vive Digital. Servicio que se presta en contra jornada.

[A.23] Manipulación de los equipos: Esta dimensión experimenta un alto grado de degradación confidencial, ya que los equipos por parte de administración, no cuentan con políticas de seguridad y el uso exclusivo no es implementado.

Identificación y valoración de amenazas: Equipamiento auxiliar

Tabla 15. Identificación y valoración de amenazas: Equipamiento auxiliar

Activo/Amenaza	Frecuencia	Dimensión de seguridad				
		D	I	C	A	T
[I.5] Avería de origen físico y lógico.	PF	A				

Fuente: autor

Justificación de amenazas – Equipamiento auxiliar

[I.5] Avería de origen físico y lógico: Se valoró la dimensión disponibilidad en alto, debido a que no se cuenta con gabinetes para *routers, switch* y *cables*.

Identificación y valoración de amenazas: Instalaciones

Tabla 16. Identificación y valoración de amenazas: Instalaciones

Activo/Amenaza	Frecuencia	Dimensión de seguridad				
		D	I	C	A	T
[A.26] Ataque destructiva	PF	A				

Fuente: autor

Justificación y valoración – Instalaciones

[A.26] Ataque destructiva: Se considera ésta dimensión como alta, ya que no se cuentan con gabinetes, quedando expuestos y sin ninguna seguridad los equipos, por lo que cualquier persona puede tener acceso a estos.

Identificación y valoración de amenazas: Personal

Tabla 17. Identificación y valoración de amenazas: Personal

Activo/Amenaza	Frecuencia	Dimensión de seguridad				
		D	I	C	A	T
[E.7] Deficiencia en la organización.	FN	A				
[E.15] Alteración accidental de la información.	FN		A	A		
[E.30] Ingeniería social.	F	A	A	A		

Fuente: autor

Justificación y valoración – Personal

[E.7] Deficiencia en la organización: Se valoró como una degradación alta, porque no cuenta con personal calificado para implementar el Sistema de Gestión de Seguridad Informática, que se deben realizar en la institución educativa departamental Luis Carlos Galán, además no se cuenta con un cronograma de actividades para el manteniendo de equipos de cómputo en la institución.

[E.15] Alteración accidental de la información: Esta amenaza cuenta con una frecuencia de normal, donde su dimensión es valorada en la integridad de los datos y la confidencialidad de la información en alto, debido a la falta de capacitación y al desconocimiento de temas de seguridad informática.

[E.30] Ingeniería social: Se valoró con una frecuencia alta, al igual que sus dimensiones de disponibilidad, integridad de los datos y confidencialidad, debido a que el personal docente al momento del ingreso de las notas no las realizan ellos mismo, sino personas externas a la institución, no siendo conscientes del valor que tiene dicha información.

Este diagnóstico se realizó por medio de entrevista, al jefe de sistemas administrativo de la institución Luis Carlos Galán, y de encuesta aplicada. (Ver Anexo B)

7.5.2.3 Evaluación de las salvaguardas. La evaluación de los salvaguardas son llamadas también contramedidas, las cuales permiten hacer frente a las amenazas, para ello es importante implementar normas que tengan que ver con aspectos organizativos, técnicos, físicos y gestión personal, mecanismos de seguridad física y lógica. Si se realiza las debidas salvaguardas, el impacto, la probabilidad y el riesgo se mitigan, viéndose reducidos a valores residuales.

De acuerdo a lo anterior, los activos incluidos en el análisis de riesgos de la institución educativa departamental Luis Carlos Galán, estarán basados en el catálogo de elementos que proporciona *Magerit v3.0*.

Salvaguarda activos: protecciones generales u horizontales

Tabla 18. Salvaguarda activos: protecciones generales u horizontales

Salvaguarda	Dimensiones	Evaluación
Control de acceso lógico	[A], [D], [C]	20%
IDS/IPS Detección y prevención de intrusión	[C], [I], [A], [D]	50%

Fuente: autor

Descripción del salvaguarda control de acceso lógico: Actualmente el acceso a servicios web se realizan por medio de autenticación de usuarios, esta sería una salvaguarda que logra proteger los activos del tipo servicios en la dimensión disponibilidad, confidencialidad y autenticidad de los usuarios del servicio, dándole una evaluación del 20%, debido a que estos mecanismos de seguridad básicos, no son los ideales, y altamente vulnerables.

IDS/IPS Detección y prevención de intrusión: Este módulo protege los posibles intentos de acceso no autorizado desde internet, igualmente en la red inalámbrica protegiéndola al acceso de los servicios, en las dimensiones de confidencialidad, integridad, autenticidad y disponibilidad. La valoración dada de 50%, surge de las reglas establecidas ya que son vulnerables, debido a las necesidades que tiene la institución.

Salvaguardas activos: Protección de los datos/información

Tabla 19. Salvaguardas activos: Protección de los datos/información

Salvaguarda	Dimensiones	Evaluación
Copias de seguridad de los datos (*Backup*)	[I], [A], [C], [D], [T]	10%
Uso de firmas electrónicas.	[C], [T], [A], [I]	30%

Fuente: autor

Descripción del salvaguarda copia de seguridad de los datos: El sistema de salvaguarda utilizado por la institución para tener copias de seguridad de su sistema, es manejado por un sistema externo, Sistema Integrado de Matricula (SIMAT), comprendiendo varios aspectos que cubren el control de acceso y los servicios de seguridad, manejando un esquema de autorización del sistema comprende la definición de roles y privilegios de cada uno de los usuarios. Su

evaluación es baja ya que se presentan fallas de software, liberación de alumnos, alumnos en otros estados y en otras vigencias, entre otros).

El sistema de información para la gestión escolar, SIGES que es utilizado como mecanismo de evaluación, que se ajusta a la metodología de la institución. Su asistencia técnica se realiza a través de soporte técnico de la dirección de medios y nuevas tecnologías de la secretaria de educación de Cundinamarca.

Descripción de la salvaguarda del uso de firmas electrónicas: Actualmente cuenta con una aplicación de certificación electrónica el cual es utilizado para la autenticidad, confidencialidad, integridad y trazabilidad de la información. Su valoración es debido a que no siempre es utilizado este mecanismo y crea irregularidades en el manejo.

Salvaguarda activos: Protección de los servicios

Tabla 20. Salvaguarda activos: Protección de los servicios

Salvaguarda	Dimensiones	Evaluación
Se aplican perfiles de seguridad.	[A], [I], [D]	60%
Protección de servicios y aplicaciones web.	[I],[D]	60%

Fuente: autor

Descripción de la salvaguarda de perfiles de seguridad: Son aplicados a través de políticas de *firewall* y software de seguridad antivirus-antispyware, sistemas operativos tipo servidor. Su aplicación está orientada a las dimensiones de autenticidad, integridad de los datos y disponibilidad de la información, su valoración es aceptable, ya que es uno de las salvaguardas más importantes.

Descripción del salvaguarda de protección de servicios y aplicaciones web: El servicio de protección que presta las aplicaciones web a la comunidad académica y administrativa de la secretaria de educación de Cundinamarca y Nacional, tiene salvaguardas, con herramientas de autenticación básicas, aunque su evaluación es aceptable, puede mejorar en los procesos de cifrar las contraseñas, ya que la integridad y disponibilidad del sistema es vulnerable.

Salvaguardas activos: Protección de las aplicaciones (Software)

Tabla 21. Salvaguardas activos: Protección de las aplicaciones (Software)

Salvaguarda	Dimensiones	Evaluación
Cambios (Actualizaciones y mantenimiento)	[I],[D], [T]	70%

Fuente: autor

Descripción del salvaguarda de cambios (Actualizaciones y mantenimiento): La evaluación que se le da es debido a que las actualizaciones y mejoras que se les ha hecho a estos sistemas han estado acorde a las necesidades esperadas, pero a un falta mejorar en los procesos.

Salvaguarda activos: Protección de los equipos (Hardware)

Tabla 22. Salvaguarda activos: Protección de los equipos (Hardware)

Salvaguarda	Dimensiones	Evaluación
Operación	[D]	40%
Cambios (Actualizaciones y mantenimiento)	[D], [T]	40%

Fuente: autor

Descripción del salvaguarda de operación: El uso de los equipos de cómputo se realiza de acuerdo a las necesidades durante la jornada escolar, por la institución, por el SENA y en jornada contraria se habilita el servicio del Kiosco vive digital, el cual ofrece un servicio a nivel de la comunidad. Su evaluación obedece a que no se tiene definido un procedimiento de buenas prácticas, de acuerdo al trato del equipamiento en general.

Descripción del salvaguarda cambios (Actualizaciones y mantenimiento): El mantenimiento y actualización que se realizan de acuerdo a la programación planteada por la institución y el SENA, ofreciendo a los aprendices la formación en mantenimiento preventivo, predictivo y correctivo, garantizando el funcionamiento del hardware de los equipos. Por esta razón se relacionan con la dimensión de disponibilidad y trazabilidad.

Salvaguardas activos: Protección de las comunicaciones.

Tabla 23. Salvaguardas activos: Protección de las comunicaciones.

Salvaguarda	Dimensiones	Evaluación
Internet: ¿Uso de? ¿Acceso a?	[D], [C],[T]	40%
Seguridad Wireless (Wifi)	[D], [C]	40%

Fuente: autor

Descripción del salvaguarda del Internet: ¿Uso de? ¿Acceso a?: Actualmente no se controla el sistema de monitoreo, como tampoco se gestiona el tráfico y disponibilidad de ancho de banda, en cambio sí se realizan restricciones a accesos a sitios específicos. La evaluación de salvaguarda es baja por lo que no se cumple completamente.

Descripción del salvaguarda de la seguridad Wireless (Wifi): Actualmente existe una red inalámbrica en la institución, la cual realiza un control de acceso a los usuarios. La evaluación del salvaguarda es baja, debido a que no cuenta con un control de protocolos de entrada y salida, no se aplica control en el ancho de banda y no se cuenta con un escaneo de virus.

Tabla 24. Identificación de amenazas

Activos	Amenazas
INTERNET	[A.1] Uso no previsto
OFIMÁTICA	[E.1] Errores de usuario. [E.2] Vulnerabilidades de los programas [E.2] Errores de mantenimiento / actualización de programas. [A.3] Difusión de software dañino.
ANTIVIRUS	[E.2] Difusión de software dañino [E.3] Vulnerabilidades de los programas [E.2] Errores de mantenimiento / actualización de programas.
SISTEMA OPERATIVO	[I.2] Avería de origen físico y lógico [E.1] Errores de usuario. [E.2] Difusión de software dañino. [E.3] Vulnerabilidades de los programas [E.3] Errores de mantenimiento / actualización de programas. [A.3] Uso no previsto

Identificación de amenazas (Continuación)

Activos	Amenazas
OTROS SOFTWARE	[E.3] Difusión de software dañino [E.3] Vulnerabilidades de los programas. [E.3] Errores de mantenimiento /actualización de programas.
SERVIDOR DE BASE DE DATOS	[N.1] Fuego [N.1] Daños por agua [N.1] Desastres naturales [I.1] Contaminación medio ambiental [I.2] Avería de físico y lógico. [I.1] condiciones inadecuadas de temperatura o humedad. [E.2]Errores del administrador del sistema / de la seguridad. [E.1] Errores de mantenimiento /actualización de equipos. [A.3] Acceso no autorizado [A.2] Manipulación del hardware
MEDIOS DE IMPRESIÓN	[I.2] Avería de físico o lógico [I.2] Condiciones inadecuadas de temperatura o humedad. [E.2] Errores de mantenimiento. [A.2] Acceso no autorizado
COMPUTADORAS	[N.1] Daños por agua [N.1] Desastres naturales [I.1] Desastres industriales [I.3] Averías de origen físico o lógicos [I.1] Condiciones inadecuadas de temperatura o humedad. [E.1] Errores de mantenimiento / actualización de equipos. [E.1] Caída del sistema por agotamiento de recursos. [A.2] Abuso de privilegios de accesos [A.2] Uso no previsto
ROUTER	[N.1] Fuego [N.1] Dalos por agua [N.1] Desastres naturales [I.1] Contaminación medioambiental [I.1] Condiciones inadecuadas de temperatura o humedad. [E.1] Errores de mantenimiento / actualización de equipos. [A.2] Acceso no autorizado

Identificación de amenazas (Continuación)

Activos	Amenazas
RED WIFI	[I.3] Fallo de servicio de comunicación [E.3] Acceso no autorizado [E.3] Errores de [re-] encaminamiento
RED LAN	[I.3] Fallo de servicios de comunicaciones [E.3] Errores de [re-] encaminamiento [E.3] Errores de secuencias [A.2] Suplantación de identidad del usuario [A.3] Acceso no autorizado
INTERNET	[A.3] Fallo de servicios de comunicación [A.3] Alteración de la información
CABLEADO	[I.1] Contaminación medio ambiental [I.1] Condiciones inadecuadas de temperatura.
MOBILIARIO	[I.1] Contaminación medio ambiental
SISTEMAS DE VIGILANCIA	[I.1] Contaminación medio ambiental [I.1] Condiciones inadecuadas de temperatura.
ANTENAS	[I.1] Contaminación medio ambiental
OTROS EQUIPOS AUXILIARES	[I.1] Contaminación medio ambiental
CD	[E.3] Alteración de la información [E.3] Fugas de información [A.3] Modificación de la información [A.3] Revelación de la información
DISCO EXTRAÍBLE	[E.3] Alteración de la información [E.3] Fugas de información [A.3] Modificación de la información [A.3] Revelación de la información
COLEGIO	[N.1] Fuego [N.1] Daños por agua [N.1] Tormentas [N.1] Terremotos [N.1] calor extremo [I.1] Desastres industriales
MANTENIMIENTO DE BASES DE DATOS	[E.2] Errores de configuración
SECRETARIA	[E.2] Enfermedad [E.2] Huelga [E.2] Extorsión [E.2] Ingeniería social
COORDINADOR	[E.2] Enfermedad [E.2] Huelga

Identificación de amenazas (Continuación)

Activos	Amenazas
COORDINADOR	[E.2] Extorsión [E.2] Ingeniería social
RECTOR	[E.2] Enfermedad [E.2] Huelga [E.2] Extorsión [E.2] Ingeniería social
JEFE DE SISTEMA ADMINISTRATIVOS	[E.2] Enfermedad [E.2] Huelga [E.2] Extorsión [E.2] Ingeniería social
SOPORTE	[E.2] Enfermedad [E.2] Huelga [E.2] Extorsión [E.2] Ingeniería social

Fuente: autor

Valoración de las amenazas

Los objetivos planteados en esta actividad son:

- Evaluar la probabilidad de ocurrencia de cada amenaza concerniente a cada activo.
- Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse.

Las tablas 30 y 31 valoran cada activo teniendo en cuenta la degradación de valor y la probabilidad de ocurrencia.

Cuadro 3: Degradación del valor

A	ALTA
M	MEDIA
B	BAJA
0	

Fuente: autor

Cuadro 4: Probabilidad de ocurrencia

CS	CASI SEGURO
MA	MUY ALTO
P	POSIBLE
PP	POCO PROBABLE
O	

Fuente: autor

Tabla 25. Valoración de amenazas de cada uno de los activos

ACTIVOS	AMENAZAS	Probabilidad de ocurrencia	[D]	[I]	[C]	[A]	[T]
INTERNET	Uso no previsto	PP	M	-	-	-	-
OFIMÁTICA	Errores de los usuarios	P	M	M	M	-	-
	Vulnerabilidades de los programa (Software)	P	M	M	M	-	-
	Errores de mantenimiento / Actualización de programas (Software)	P	M	B	-	-	-
	Difusión de software dañino	PP	B	B	B	-	-
ANTIVIRUS	Difusión de software dañino	PP	B	B	B	-	-
	Vulnerabilidades de los programa (Software)	P	M	M	M	-	-
	Errores de mantenimiento / Actualización de	P	M	M	-	-	-
ANTIVIRUS	programas (Software)						
OPERATIVO	Avería de origen físico o lógico	P	M	-	-	-	-
	Errores de los usuarios	PP	M	M	M	-	-
	Difusión de software dañino	PP	B	B	B	-	-
	Vulnerabilidades de los programas (Softwa)	P	B	M	M	-	-
	Errores de mantenimiento / Actualización de programas (Software)	P	M	B	-	-	-
	Uso no previsto	P	B	B	B	-	-

Valoración de amenazas de cada uno de los activos

ACTIVOS	AMENAZAS	Probabilidad de ocurrencia	[D]	[I]	[C]	[A]	[T]
OTROS SOFTWARE	Difusión de software dañino	PP	B	B	B	-	-
	Vulnerabilidades de los programas (Software)	PP	B	B	B	-	-
	Errores de mantenimiento / Actualización de programas (Software)	P	M	B	-	-	-
SERVIDOR DE BASES DE DATOS	Fuego	P	A	-	-	-	-
	Daños por agua	P	A	-	-	-	-
	Desastres naturales	P	A	-	-	-	-
	Contaminación medio ambiental	P	A	-	-	-	-
	Avería de origen físico o lógico	P	A	-	-	-	-
SERVIDOR DE BASES DE DATOS	Errores del administrador del sistema de seguridad	P	M	M	M	-	-
	Condiciones inadecuadas de temperatura o humedad	MA	MA	-	-	-	-
SERVIDOR DE BASES DE DATOS							
	Acceso no autorizado	MA	-	A	A	-	-
	Manipulación del hardware	MA	A	-	A	-	-
MEDIOS DE IMPRESIÓN	Avería de origen físico o lógico	P	M	-	-	-	-
	Condiciones inadecuadas de temperatura o humedad	P	M	-	-	-	-
	Errores de mantenimiento / Actualización de programas (Hardware)	P	M	-	-	-	-
	Acceso no autorizado	PP	-	M	M	-	-

Valoración de amenazas de cada uno de los activos

ACTIVOS	AMENAZAS	Probabilidad de ocurrencia	[D]	[I]	[C]	[A]	[T]
COMPUTADORES	Daños por agua	PP	M	-	-	-	-
	Desastres naturales	PP	M	-	-	-	-
	Desastres industriales	P	B	-	-	-	-
	Averías de físico o lógico	P	M	-	-	-	-
	Condiciones inadecuadas de temperatura o humedad	PP	M	-	-	-	-
	Errores de mantenimiento / actualización de equipos (Hardware)	P	M	-	-	-	-
	Caída del sistema por agotamiento del recurso	P	M	-	-	-	-
	Abuso de privilegios de acceso	PP	M	M	M	-	-
	Uso no previsto	P	M	B	M	-	-
SERVIDOR DE BASES DE DATOS	Errores del administrador del sistema de seguridad	P	M	M	M	-	-
	Condiciones inadecuadas de temperatura o humedad	MA	MA	-	-	-	-
	Acceso no autorizado	MA	-	A	A	-	-
	Manipulación del hardware	MA	A	-	A	-	-
MEDIOS DE IMPRESIÓN	Avería de origen físico o lógico	P	M	-	-	-	-
	Condiciones inadecuadas de temperatura o humedad	P	M	-	-	-	-
	Errores de mantenimiento / Actualización de programas (Hardware)	P	M	-	-	-	-
	Acceso no autorizado	PP	-	M	M	-	-

Valoración de amenazas de cada uno de los activos

ACTIVOS	AMENAZAS	Probabilidad de ocurrencia	[D]	[I]	[C]	[A]	[T]
COMPUTADORES	Daños por agua	PP	M	-	-	-	-
	Desastres naturales	PP	M	-	-	-	-
	Desastres industriales	P	B	-	-	-	-
	Averías de físico o lógico	P	M	-	-	-	-
	Condiciones inadecuadas de temperatura o humedad	PP	M	-	-	-	-
	Errores de mantenimiento / actualización de equipos (Hardware)	P	M	-	-	-	-
	Caída del sistema por agotamiento del recurso	P	M	-	-	-	-
	Abuso de privilegios de acceso	PP	M	M	M	-	-
	Uso no previsto	P	M	B	M	-	-
ROUTER	Fuego	PP	M	-	-	-	-
	Daños por agua	PP	M	-	-	-	-
	Desastres naturales	PP	M	-	-	-	-
	Contaminación medio ambiental	PP	M	-	-	-	-
	Avería de origen físico o lógico	P	M	-	-	-	-
	Condiciones inadecuadas de temperatura o humedad	P	M	-	-	-	-
	Acceso no autorizado	PP	-	B	B	-	-
RED WIFI	Fallo de servicio de comunicación	P	M	-	-	-	-
	Errores de reencaminamiento	P	-	-	B	-	-
RED LAN	Fallo de servicio de comunicaciones	PP	B	-	-	-	-
	Errores de re-encaminamiento	P	-	-	M	-	-

Valoración de amenazas de cada uno de los activos

ACTIVOS	AMENAZAS	Probabilidad de ocurrencia	[D]	[I]	[C]	[A]	[T]
	Errores de secuencia	P	-	M	-	-	-
	Suplantación de la identidad del usuario	P	-	M	M	M	-
	Re-encaminamiento de mensajes	P	-	-	M	-	-
	Alteración de secuencias	P	-	M	-	-	-
	Acceso no autorizado	PP	-	M	-	-	-
INTERNET	Fallo de servicio de comunicación	P	A	-	-	-	-
	Alteración de la información	P	-	B	-	-	-
CABLEADO	Contaminación medioambiental	PP	A	-	-	-	-
	Contaminación electromagnética	MR	B	-	-	-	-
MOBILIARIO	Contaminación medioambiental	PP	M	-	-	-	-
SISTEMA DE VIGILANCIA	Condiciones inadecuadas de temperatura o humedad	MA	A	-	-	-	-
ANTENAS	Contaminación medioambiental	PP	A	-	-	-	-
OTROS EQUIPOS AUXILIARES	Contaminación medioambiental	P	M	-	-	-	-
CD	Alteración de información	PP	-	B	-	-	-
	Fugas de información	PP	-	-	B	-	-
	Modificación de la información	PP	-	B	-	-	-
	Revelación de información	PP	-	-	B	-	-
DISCO EXTRAÍBLE	Alteración de información	PP	-	B	-	-	-
	Fugas de información	PP	-	-	B	-	-
	Modificación de la información	PP	-	B	-	-	-
	Revelación de información	PP	-	-	B	-	-

Valoración de amenazas de cada uno de los activos

ACTIVOS	AMENAZAS	Probabilidad de ocurrencia	[D]	[I]	[C]	[A]	[T]
COLEGIO	Fuego	P	A	-	-	-	-
	Daños por agua	P	A	-	-	-	-
	Desastres naturales	P	A	-	-	-	-
	Terremotos	P	M	-	-	-	-
COLEGIO	Calor extremo	MA	B	-	-	-	-
	Desastres industriales	P	B	-	-	-	-
SECRETARIA	Enfermedad	P	M	M	M	-	-
	Huelga	PP	B	-	-	-	-
	Extorción	PP	M	M	M	-	-
	Ingeniería social	MA	A	A	B	-	-
MANTENIMIENTO BASE DE DATOS	Errores de configuración	P	-	A	-	-	-
	A personas externas que no necesitan conocerlos	P	-	-	A	-	-
	Ataques desde el interior	P	M	M	M	-	-
COORDINADOR	Enfermedad	P	M	M	M	-	-
	Huelga	PP	B	-	-	-	-
	Extorción	PP	M	M	M	-	-
	Ingeniería social	MA	A	A	B	-	-
RECTOR	Enfermedad	P	M	M	M	-	-
	Huelga	PP	B	-	-	-	-
	Extorción	PP	M	M	M	-	-
	Ingeniería social	MA	A	A	B	-	-
JEFE DE SISTEMAS ADMINISTRATIVOS	Enfermedad	P	M	M	M	-	-
	Huelga	PP	B	-	-	-	-
	Extorción	PP	M	M	M	-	-
	Ingeniería social	MA	A	A	B	-	-
SOPORTE	Enfermedad	P	M	M	M	-	-
	Huelga	PP	B	-	-	-	-
	Extorción	PP	M	M	M	-	-
	Ingeniería social	MA	A	A	B	-	-
RECTOR	Enfermedad	P	M	M	M	-	-
	Huelga	PP	B	-	-	-	-
	Extorción	PP	M	M	M	-	-
	Ingeniería social	MA	A	A	B	-	-
JEFE DE SISTEMAS ADMINISTRATIVOS	Enfermedad	P	M	M	M	-	-
	Huelga	PP	B	-	-	-	-
	Extorción	PP	M	M	M	-	-
	Ingeniería social	MA	A	A	B	-	-

Valoración de amenazas de cada uno de los activos

ACTIVOS	AMENAZAS	Probabilidad de ocurrencia	[D]	[I]	[C]	[A]	[T]
SOPORTE	Enfermedad	P	M	M	M	-	-
	Huelga	PP	B	-	-	-	-
	Extorción	PP	M	M	M	-	-
	Ingeniería social	MA	A	A	B	-	-
RECTOR	Enfermedad	P	M	M	M	-	-
	Huelga	PP	B	-	-	-	-
	Extorción	PP	M	M	M	-	-
	Ingeniería social	MA	A	A	B	-	-
JEFE DE SISTEMAS ADMINISTRATIVOS	Enfermedad	P	M	M	M	-	-
	Huelga	PP	B	-	-	-	-
	Extorción	PP	M	M	M	-	-
	Ingeniería social	MA	A	A	B	-	-
SOPORTE	Enfermedad	P	M	M	M	-	-
	Huelga	PP	B	-	-	-	-
	Extorción	PP	M	M	M	-	-
	Ingeniería social	MA	A	A	B	-	-

Fuente: autor

7.5.3 Proceso P3: Estimación del estado de riesgo. La siguiente actividad se realizó con el propósito de analizar los datos compilados de las actividades anteriores y así evaluar el estado de riesgo, determinando el impacto y el riesgo.

Estimación del Impacto. Es denominado como la medida del daño sobre el activo. A su vez se mide el valor de los activos y la degradación que son causantes de las amenazas, provocando un impacto directo que tendrían sobre el sistema.

Tabla 26. Impacto potencial sobre cada uno de los activos

ACTIVOS	[D]	[I]	[C]	[A]	[T]
Servicios internos					
Internet	[2]	[3]	[3]		
Equipamiento					
Aplicaciones					
Ofimática		[3]	[3]		
Antivirus		[3]	[3]		
Sistema Operativo		[3]	[3]		

Impacto potencial sobre cada uno de los activos (continuación)

ACTIVOS	[D]	[I]	[C]	[A]	[T]
Otros software		[3]	[3]		
Equipos					
Servidor de bases de datos		[3]	[3]		
Medios de impresión		[2]	[2]		
Computadores		[2]	[2]		
Router		[1]	[1]		
Comunicación					
Red Wifi			[2]		
Red Lan		[2]	[3]	[2]	
Internet		[2]			
Elementos auxiliares					
Cableado	[2]				
Mobiliario	[2]				
Sistemas de vigilancia	[2]				
Antenas	[2]				
Otros equipos auxiliares	[1]				
Soportes de información					
CD		[1]	[1]		
Discos extraíbles		[1]	[1]		
Instalaciones					
Colegio			[3]		
Personal					
Rector			[2]		
Coordinador			[2]		
Secretaria			[3]		
Jefe de sistemas administrativos			[2]		
Soporte			[2]		

Fuente: autor

Impacto Residual Acumulado. Se calcula con los datos del impacto acumulado sobre un activo apropiado para las amenazas de dicho activo.

Tabla 27. Impacto potencial sobre cada uno de los activos

ACTIVOS	[D]	[I]	[C]	[A]	[T]
Servicios internos					
Internet	[1]	[5]	[5]		
Equipamiento					
Aplicaciones					

Impacto potencia sobre cada uno de los activos (continuación)

ACTIVOS	[D]	[I]	[C]	[A]	[T]
Ofimática		[1]	[1]		
Antivirus		[0]	[0]		
Sistema Operativo		[1]	[1]		
Otros software		[1]	[1]		
Equipos					
Servidor de bases de datos		[1]	[1]		
Medios de impresión		[1]	[1]		
Computadores		[1]	[2]		
Router		[0]	[0]		
Comunicación					
Red Wifi			[1]		
Red Lan		[1]	[3]	[2]	
Internet		[2]			
Elementos auxiliares					
Cableado	[2]				
Mobiliario	[1]				
Sistemas de vigilancia	[1]				
Antenas	[1]				
Otros equipos auxiliares	[1]				
Soportes de información					
CD		[1]	[1]		
Discos extraíbles		[1]	[1]		
Instalaciones					
Colegio			[3]		
Personal					
Rector			[1]		
Coordinador			[1]		
Secretaria			[2]		
Jefe de sistemas administrativos			[1]		
Soporte			[1]		

Fuente: autor

7.6 HALLAZGOS ENCONTRADOS

Con los activos más importantes previamente identificados se ha realizado un diagnóstico al sistema de red y se ha podido identificar los riesgos de acuerdo a los resultados obtenidos teniendo en cuenta las necesidades y característica de cada activo:

Hardware:

- La institución cuenta con personal para realizar el mantenimiento preventivo, correctivo en los equipos de la institución, pero la programación que se realiza no se cumple según lo planeado.

- Los procedimientos realizados en el mantenimiento correctivo y preventivo, no son normalizados los procedimientos técnicos, provocando que la solución no sea la más efectiva o la más eficaz.

- No existen restricciones para el uso de dispositivos de almacenamiento tipo USB, provocando la infección fácilmente en el sistema.

- Si se presenta una falla irrecuperable de hardware en un equipo de cómputo de uso crítico, no se cuenta con planes de contingencias que permitan hacer un proceso de recuperación que se pueda comprometer.

Software

- No se tiene implementado un resguardo de los datos que permitan recuperar la continuidad del negocio ante una contingencia, dado que no se realizan copias de seguridad periódicamente.

- Se tiene un servicio ocasional de soporte contratado con un tercero para atender las eventualidades que se presenten.

- No se cuenta con procedimientos definidos, ni registro de aplicación de actualizaciones de software o parches de seguridad en los sistemas base críticos.

Redes

- No se realiza un monitoreo al sistema que permita identificar amenazas internas o externas, lo que no permite prevenir situaciones críticas que puedan suceder o identificar si se está siendo vulnerado el sistema, situación que puede estar sucediendo dado que hay momentos en los cuales la navegabilidad se pone muy lenta, a pesar de contar con un ancho de banda suficiente para los procesos que se realizan en la red.

- La red Wifi presenta alta vulnerabilidad, dado que los estudiantes y parte de la comunidad alrededor de la institución se conectan permanentemente, debido a la falta de restricciones.

- La vulnerabilidad de la red, permite el desarrollo de Ingeniería social sobre los usuarios de la misma.

Instalaciones físicas

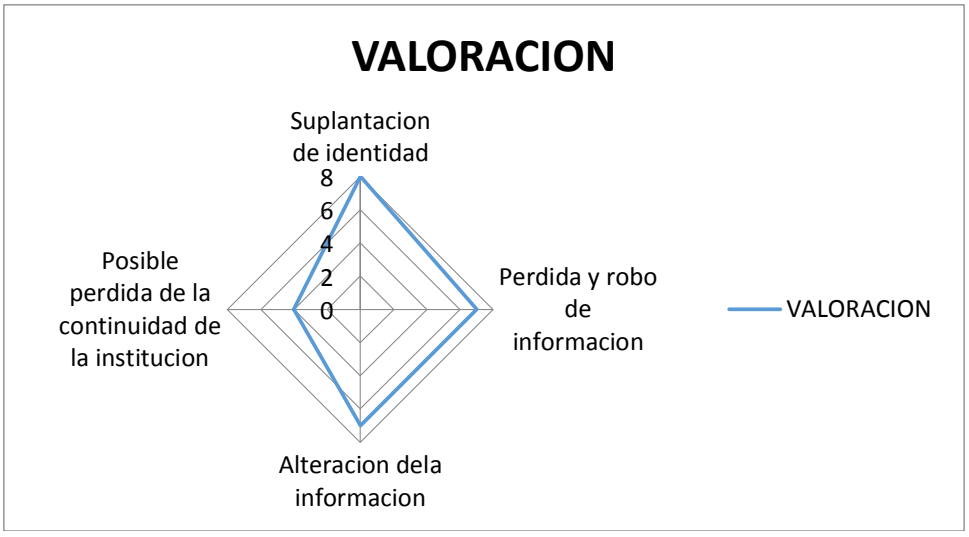
- El estado del cableado estructurado encontrado en la sede principal son de tipo UTP categoría 6 de los cuales no cumplen con las normas mínimas de instalación, como son el caso de los armarios de cableados, patch-panel y patch-cord donde se encuentran desorganizados y en malas condiciones, como también se encontró que cualquier persona tiene acceso a dichos recursos provocando así inseguridad.

- Las condiciones ambientales y de seguridad que presenta la institución en la sede principal son las siguientes: no cuenta con un sistema inteligente de prevención contra incendios, no siempre se encuentran los sistemas de aires acondicionados encendidos, no existe restricción al acceso a estos lugares.

Consecuencias

- Suplantación de identidad.
- Pérdida y robo de información.
- Alteración de la información.
- Posible pérdida de la continuidad del servicio.

Figura 16. Valoración suplantación de identidad



Fuente: autor

7.7 CONTROLES

Definir políticas de seguridad para la red de la institución educativa y diseñar un paquete que de soluciones para establecer y mantener la seguridad de la información de modo que se pueda garantizar la continuidad del servicio ante algún evento, donde se incluya entre otros aspectos:

- Segmentar la red al nivel de oficinas

- Realizar la configuración del *Firewall*, aislando la red externa con la red interna para los terminales.

- Configurar parámetros de seguridad del *Routers*, realizando una encriptación segura.

- Definir usuarios, determinando niveles de acceso.

- Restringir el servicio en horarios no laborales.

- Capacitación de personal.

- Establecer una estrategia de resguardo de los datos ya sea a través de un proceso de soporte interno o externo.

- Implementar un servicio de soporte preventivo que permita identificar y atender posibles vulnerabilidades y amenazas.

- Implementar un servicio de monitoreo a la red con una herramienta como *AutoScan Network* que identifique si se está tratando de vulnerar la seguridad por parte de intrusos externos.

Implementación del plan de mitigación. Finalizada la evaluación del riesgo, se ejecutan las medidas correctivas, donde se escoge una serie de opciones para mitigar el riesgo, estos procesos son repetitivos, determinado así su tolerabilidad en contra de los criterios establecidos, con el fin de decidir si se debe aplicar un tratamiento posterior. Cuando los riesgos superan los umbrales son monitoreados, aplicando los planes de mitigación de riesgos devolviendo el esfuerzo efectuado a un nivel de riesgo aceptable. De no ser mitigado el riesgo se procede a implementar un plan de contingencia.

Aceptar el riesgo. En este punto la encargada de determinar el nivel de riesgo es la dirección de la organización, teniendo en cuenta las consecuencias que estas puedan alcanzar. Aceptar el riesgo es asumir responsabilidades frente a las insuficiencias encontradas de un riesgo residual.

Control de seguimiento y monitoreo del riesgo tratado. Los riesgos y los controles deben ser monitoreados y revisados periódicamente comprobando la hipótesis sobre los riesgos.

Controles de acceso físico. Se deben asignar sitios seguros para el sector de comunicaciones y servidores y para el acceso físico se establecerán controles que permitan solo el ingreso de personal autorizado.

Seguridad del cableado. Los cables de comunicaciones y energía estarán respaldados a través de una UPS, el cual brindará apoyo a los servicios de información por un tiempo prudencial.

Mantenimiento de equipos. El mantenimiento preventivo que se le realizará a los equipos, serán programados por la institución, mediante jornadas educativas con el apoyo del SENA.

Controles contra software malicioso. Se definirán controles de detección y prevención por parte del comité de sistemas que tiene establecida la institución, contra software malicioso, designado a personal para dichos roles.

Control de redes. Se definirá controles que garanticen la seguridad de la infraestructura de la red de la institución, previniendo el acceso no autorizado.

Estos se realizaran por medio de controles que limiten la capacidad de conexiones de los usuarios, implementándose en los *firewall*. Se incorporaran controles de ruteo, con el objetivo de no violar las políticas de control de acceso.

Controles criptográficos. Para el resguardo de la información, se utilizan claves de acceso a sistemas, datos y servicio, durante el proceso de *backups*.

Seguridad de los procesos de desarrollo y soporte. Se realizan controles durante la implementación de cambios comprobando el desempeño del procedimiento establecido.

Los cambios que se realicen a los sistemas operativos por motivos necesarios o solicitados para prácticas del SENA, serán revisados para asegurar que no produzca un impacto en su funcionamiento o seguridad. Estas actividades serán monitoreadas por personal administrativo del área de sistemas.

7.7.1 Mecanismos de control de activos

Seguridad física y ambiental. Para el correcto funcionamiento del equipamiento informático se deberán establecer controles de factores ambientales.

Controles de acceso físico. El acceso a los cuartos de comunicaciones se determinara mediante los controles de acceso físico, permitiendo así solo el ingreso a personal autorizado. Las autorizaciones estarán definidas por el comité de seguridad informática.

Protección de oficinas, recintos e instalaciones. Se determinaran las áreas más expuestas a daños producidos por incendios, explosión, inundación u otras formas de desastres naturales o provocados por el hombre teniendo en cuenta los estándares en materia de sanidad y seguridad.

Desarrollo de tareas en áreas protegidas. Para la seguridad en las áreas protegidas se establecerán controles para el personal en dicha área, de igual forma para las actividades de terceros que participen allí.

Seguridad en el cableado. Se deberán establecer mejoras en las instalaciones del cableado; a su vez el cableado de energía eléctrica y de comunicaciones estará respaldado a través de UPS.

Mantenimiento de equipos. Los mantenimientos preventivos y correctivos estarán sujetos a los intervalos de servicios y especificaciones recomendadas por el proveedor y autorización del comité de sistemas.

Controles contra software malicioso. Los controles serán determinados por el comité de sistemas y de seguridad informática, realizando la detección y prevención para la protección contra software malicioso y el personal designado elegido por dicho comité.

Controles de redes. Los controles serán definidos por el área de las TIC que garantizara la seguridad en el área de la infraestructura de comunicaciones y servicios conectados a las redes de la institución. Donde los controles limitaran la capacidad de conexión de los usuarios, según políticas establecidas para tal efecto; dichos controles se implementarán en los *Firewalls*.

Se establecerán controles de ruteo, asegurando las conexiones informáticas y los flujos de información, según las políticas establecidas de control de acceso, llevando un control de verificación positiva de direcciones de origen y destino.

Administración de medios informáticos removibles. Se establecerán controles para la gestión de medios informáticos removibles de acuerdo a las políticas establecidas como discos, memorias entre otras. Estableciendo como responsable al personal designado por el comité de sistemas y seguridad informática.

Seguridad del correo electrónico. Los riesgos de seguridad presentados en los correos electrónicos, ha hecho que se planteen políticas de seguridad que indique

como minimizarlos, estableciendo medidas de seguridad para proteger la confidencialidad del correo electrónico.

Control de acceso al sistema operativo. El área de las TIC se ejecutara evaluaciones de riesgo, con el fin de determinar la metodología de protección adecuada para el acceso y uso del sistema operativo.

Procedimientos de control de terminales. Se determinaran controles al acceso de servicio de información los cuales serán establecidos por un medio seguro de conexión. Este procedimiento es llevado a cabo con el fin de minimizar el acceso no autorizado.

Identificación y autenticación de los usuarios. Se establecerá identificación a todos los usuarios de la institución para su uso personal y exclusivo, mediante una técnica adecuada que verifique la identidad de cada usuario.

Sistema de administración de contraseñas. El sistema de autenticación de contraseñas deberá tener en cuenta lo siguientes parámetros:

- Establecer el uso individual de contraseñas para determinar responsabilidades.

- Los usuarios podrán cambiar sus contraseñas e incluir un procedimiento que contemplen los errores de ingreso.

- Imponer a los usuarios cambiar las contraseñas provisorias en caso que ingresen por primera vez.

- Se registraran las últimas contraseñas utilizadas por los usuarios y así evitar la reutilización de éstas.

- En el momento de ingresar las contraseñas, evitar mostrarlas en la pantalla.

- Registrar en forma separada las contraseñas de archivos y los datos de sistema de aplicación.

- Guardar las contraseñas utilizando un algoritmo de cifrado.

- No dejar contraseñas definidas por el vendedor o de manera estándar. Tanto para software como hardware.

- Garantizar que al momento de acceder al sistema de contraseñas, no haya ningún acceso a información temporal o de transito no protegida.

Control de acceso a aplicaciones

- Se recomienda establecer restricciones al acceso de información de acuerdo a las políticas de control definidas, sobre la base de requerimiento de cada aplicación y de acuerdo al perfil solicitado, estos incluyen al personal TIC.

- Se sugiere establecer controles que validen los datos ingresados, tan cerca del punto de origen, controlando también datos permanentes y tablas de parámetros.

Controles criptográficos. Para el control de protección de claves de acceso a sistema, datos y servicio.

Se propone el control de resguardo de información, realizados en los procesos de *backups* de los sistemas de información.

Registrar el proceso de gestión de riesgos. Se motivara a llevar un historial de los incidentes, permitiendo llevar una auditoría independiente en la gestión de riesgos, garantizando una buena gerencia de riesgos.

De acuerdo a los objetivos de control sugeridos, se ha realizado la siguiente clasificación de controles, (Planteados en *COBIT*[30]).

[30]ISACA Trust in, and value from, information systems.[on línea] [consultado el 2de noviembre de 2017]. Disponible en internet: https://www.isaca.org/Pages/default.aspx

7.8 RESUMEN DE CONTROLES

Tabla 28. Clasificación de controles

OBJETIVO DE CONTROL	CONTENIDO DEL CONTROL
Política de seguridad de la información	
Documentar política de seguridad	Se elaborara un documento de políticas, el cual se debe publicar y comunicar a toda la comunidad educativa y debe ser aprobada por la institución.
Revisión de la política de seguridad de la información.	Para la realización de estas revisiones se debe aplicar en intervalos planeados o si ocurre algún cambio significativo. Para así asegurar la continua idoneidad, eficiencia y efectividad.
Organización de la seguridad de la información	
Compromiso de la institución con la seguridad de la información.	La parte administrativa de la institución debe apoyar con el modelo de seguridad de la información dentro de la institución.
Coordinación de la seguridad de la información.	Las políticas establecidas de seguridad de la información, deben ser coordinadas por representantes de las principales sedes de la institución, con sus funciones y roles.
Asignación de responsabilidades de la seguridad de la información.	Se establecerán funciones y responsabilidades de la seguridad de la información.
Acuerdos de confidencialidad.	Se deben establecer protocolos para la revisión de los requerimientos de confidencialidad establecidos por la institución para la protección de la información.
Seguridad de los recursos humanos	
Roles y responsabilidades	Se debe definir los roles y responsabilidades de seguridad a empleados, contratistas y terceros de acuerdo a las políticas de la institución.
Seguridad física y ambiental	
Perímetro de seguridad física	Se debe de proteger las áreas donde se encuentren los activos importantes de información y medios de procesamiento, por medio de perímetros de seguridad.
Seguridad oficinas	Se debe implementar modelos de seguridad física en oficinas, habitaciones y medios de comunicación.
Seguridad de computadores	
Ubicación para protección de equipos	La ubicación de los equipos debe estar en un lugar seguro libres de amenazas y peligros ambientales, como también proteger los equipos del acceso no autorizado.

Clasificación de controles (Continuación)

OBJETIVO DE CONTROL	CONTENIDO DEL CONTROL
Seguridad en el cableado	El cableado de energía y el de las telecomunicaciones, deben ser protegidos en instalaciones que cumplan con la norma de seguridad.
Mantenimiento de equipos	A los equipos se les debe realizar un correcto mantenimiento, permitiendo la disponibilidad de estos.
Protección contra software malicioso	
Controles contra software malicioso	La implementación de controles de detección, prevención y recuperación ayudaran a protegerse de códigos maliciosos
Copias de seguridad o *backup*	Se deben realizar copias de seguridad *backup* o respaldo de la información en secretaria, coordinación y rectoría.
Gestión de seguridad de redes	
Controles de red	Se deben realizar controles a las redes, para poderlas proteger de amenazas y mantener la seguridad en la información como también controlar el tráfico de red.
Seguridad de los servicios de red	Para establecer los servicios de seguridad en la red, se deben de identificar los dispositivos que se tiene, determinar los niveles de servicio y los requerimientos e incluirlos.

Fuente: autor

8. PRESENTACIÓN DE INFORME Y RESULTADOS FINALES

Durante la ejecución de la presente auditoria, desarrollada en la Institución Educativa Departamental Luis Carlos Galán, se basó en identificar todos los activos de la institución.

La realización de la auditoria se contó con un buen cronograma de actividades, los cuales ayudaron a implementar un programa detallado de cada punto que se va evaluar y/o auditar.

En la auditoria se presenta un informe del trabajo que se describe y se detalla los hallazgos encontrados en dicha auditoria y así mismo se hace una recomendación a la posible solución, presentando las recomendaciones técnicas que realiza la audición.

8.1 RECURSO AUDITADO HARDWARE

8.1.1 Situación

- El cronograma de mantenimiento no se cumple satisfactoriamente.

- Los procedimientos de mantenimiento preventivo y correctivo no son realizados correctamente.

- No existen restricciones en la utilización de dispositivos de almacenamientos tipos USB.

- No se cuenta con planes de contingencias que permitan hacer un proceso de recuperación de la información los cuales puedan comprometer a la institución.

Causas:

- No se cuenta con el apoyo de parte del sector administrativo de la institución para para cumplir con el plan de mantenimiento

- El encargado del mantenimiento a los equipos de cómputo no cumple con las normas técnicas debido a la falta de herramientas en su laboratorio.

- No hay una normatividad que restrinja o aplique medidas para el uso de los dispositivos de almacenamiento.

- Desconocimiento de planes de contingencia que le permita la recuperación del activo más importante que es la información.

Solución:

- Crear concientización del valor de los activos tecnológicos a la parte administrativa de la institución, para así poder cumplir con el plan de mantenimiento.

- Dar apoyo al equipo de mantenimiento en la consecución de herramientas para cumplir con sus objetivos programados.

- Utilizar políticas y mecanismos de restricción o medidas adecuadas como capacitaciones para el uso seguro de los dispositivos de almacenamiento USB en los equipos de cómputo de la institución.

- Implementar planes de contingencia que permita la recuperación de la información a los activos informáticos de la institución.

8.2 RECURSO AUDITADO SOFTWARE

Situación:

- No existe un plan de resguardo de los datos.

- No se cuanta con un servicio de soporte permanente.

- No se cuenta con un plan o programa de actualización de software establecido.

Causas:

- El jefe inmediato del centro de cómputo no da la debida supervisión al caso al no realizar copias de seguridad periódicamente.

- No se le da la debida importancia de mantener un soporte permanente para atender eventualidades que se presenten.

- No dan la debida importancia de mantener los diferentes software actualizados.

Solución:

- Implementar un resguardo de datos, los cuales le permita realizar copias de seguridad periódicamente y así recuperarlos y darle continuidad al servicio ante una contingencia.

- Establecer un servicio de soporte permanente contratado por un tercero para atender las eventualidades que se presenten.

- Se debe verificar que se cumplan con el plan de actualizaciones en las fechas establecidas.

8.3 RECURSO AUDITADO REDES

Situación:

- No se realiza un monitoreo al sistema que permitan identificar las amenazas internas o externas. Ya que la navegabilidad es lenta, a pesar de contar con un ancho de banda suficiente para los procesos que se realizan en la red.

- Falta de restricción a la red wifi.

- Ingeniería social.

Causas:

- El desconocimiento de aplicar estos sistemas de monitoreo sobre amenazas.

- El jefe inmediato encargado del control de la red wifi, no da la debida supervisión.

- Los usuarios no se monitorean y hacen uso indebido de las contraseñas de las redes wifi. Por falta de capacitación en seguridad informática.

Solución:

- Implementar un sistema de monitoreo que permita identificar las amenazas internas o externas, permitiéndole prevenir situaciones críticas.

- Implementar un sistema de control de restricciones a la red, que permita dar permisos a los usuarios de dicha red.

- Dar capacitaciones a los usuarios en seguridad informática, según lo establecido en los cronogramas.

8.4 RECURSO AUDITADO INSTALACIONES FÍSICAS

Situación:

- En las instalaciones de la institución de la sede principal, se determinó que el cableado estructurado es de tipo UTP de categoría 6, donde las canaletas que soportan este cableado se encuentra en malas condiciones y los armarios, *patch-panel y patch-cord*, no cumpliendo con los requisitos mínimos de instalación. De igual forma no existe restricción al acceso a estos recursos.

- Las condiciones ambientales y de seguridad que presenta la institución en la sede principal son las siguientes: no cuenta con un sistema inteligente de prevención contra incendios, no siempre se encuentran los sistemas de aires acondicionados encendidos, no existe restricción al acceso a estos lugares.

Causas:

- Falta de presupuesto e iniciativa por parte de los encargados, para el mantenimiento de la red de la institución.

- No cuenta con una política que los rija y la falta de iniciativa por parte de la administración

Solución:

- Implementar un proyecto de mantenimiento de redes que le permitan mejorar el servicio a la institución.

- Efectuar políticas que establezcan condiciones ambientales y de seguridad en la prevención de incendios, la restricción al acceso a estos lugares, entre otros.

8.5 RECURSO AUDITADO SEGURIDAD INFORMÁTICA

Situación:

- Suplantación de identidad.

- Pérdida y robo de información.

- Alteración de la información.
- Posible pérdida de la continuidad del servicio

Causas:

- No cuentan con conocimiento sobre seguridad informática en la suplantación.
- No cuentan con copias de seguridad y pocos controles al acceso a la información.
- No tiene un sistema de validación de usuarios.
- No cuentan con un sistema de respaldo de la información.

Solución

- Capacitación en los modelos de seguridad existentes.
- Crear copias de seguridad y controles de acceso a la información.
- Implementar un sistema de validación de usuarios.
- Tener un sistema de respaldo de la información.

9. POLÍTICAS DE SEGURIDAD INFORMÁTICA

De acuerdo al informe presentado a la institución, se sugiere establecer las siguientes políticas, que son de interés y aplicabilidad general en todos los niveles, como en el ámbito administrativo como en el técnico. Para ello definieron las políticas como una serie de instrucciones, normas, estándares y practicas establecidas, determinadas por la institución, garantizando la seguridad, confidencialidad y disponibilidad de los activos información.

De acuerdo con la definición de políticas de seguridad de la información, se establecen criterios de cultura de calidad, dando confiabilidad, control, medidas y patrones técnicos de administración y organización, administración y comunicación; todo ello involucrando a todo el equipo humano que está comprometido con la seguridad y el uso de los recursos informáticos.

Finalidad de la política. La política de seguridad informática, da soporte a la gestión, producción conservación, recuperación, información institucional, difusión de los documentos y conservación. Bajo las siguientes dimensiones de confiabilidad, integridad y autenticidad, siendo éstas de carácter indispensable para la gestión institucional, como garantía de la prestación del servicio de la institución galanista.

Alcance. El alcance establecido de acuerdo a las políticas de seguridad de la institución educativa departamental Luis Carlos Galán, debe estar ligada al programa de gestión documental desde la producción o recepción de documentos, direccionamiento, trámite, consulta y conservación o disposición final según lo establezca la normatividad del área de archivo. Siendo los documentos un activo estratégico para el cumplimiento misional, hasta la identificación y mitigación de riesgo.

Política de seguridad institucional. Las políticas establecidas en la gestión de recursos tecnológicos propondrán y controlara el cumplimiento de las normas y políticas de seguridad, garantizando las acciones preventivas y correctivas para la salvaguarda de los equipos e instalaciones de cómputo, así como la información automatizada en general.

Para los funcionarios nuevos de la institución Luis Carlos Galán deberán realizar la inducción sobre las políticas y estándares de seguridad informática, donde se les darán a conocer las obligaciones y sanciones que se puede incurrir en caso de no cumplirlas.

9.1 SEGURIDAD RELACIONADA AL PERSONAL

9.1.1 Funcionarios

- Los funcionarios de la institución Luis Carlos Galán, están en la obligación de preservar y proteger los registros de la infraestructura tecnológica, como también deberán proteger la información almacenada o transmitida dentro o fuera de la institución o en sedes internas o externas.

- La información utilizada como producto o manipulación por los funcionarios de la institución es considerada como propiedad de la institución Luis Carlos Galán.

- Los archivos que sean proporcionados por personal interno o externo como: programas, bases de datos, documentos u hojas de cálculo y que deban de ser descomprimidos, deberán ser escaneados por un antivirus autorizado por la institución, antes de ejecutarse para que estén libres de virus.

- A los funcionarios de la institución se les prohibirá borrar, falsificar, esconder o sustituir la identidad de un usuario de correo electrónico.

- Los funcionarios de la institución solo tendrán acceso a manipular únicamente la información que les corresponda dentro de las funciones estipuladas dentro del contrato.

- Queda prohibido divulgar información a terceros que tengan que ver con la institución.

- Se establece que la información de la institución es exclusiva y ningún funcionario tiene derecho a ella.

- Los usuarios de la red de la institución Luis Carlos Galán, deberán regirse a las normas y políticas de seguridad informática establecidas.

- Es responsabilidad del usuario del manejo de la información personal y la manipulación de los equipos de cómputo y red institucional.

9.1.2 Capacitación

- Para la realización de capacitación de personal interno o externo, se deben tomar medidas de seguridad, donde no se comprometan los activos de información, para ello se deberán realizar las capacitaciones de prueba y/o simuladores.

- Todo personal que haga uso de la red de datos, deberá ser capacitado en temas de seguridad de la información, como también en las áreas específicas que tenga una función encomendada.

- El grupo de las TIC se encargara de establecer un equipo especializado en seguridad informática el cual se encargara de realizar las capacitaciones en cada dependencia.

- Se deberá establecer un cronograma de capacitaciones, el cual estará dirigido por el personal del equipo de seguridad informática.

- Dichas capacitaciones deberán contar con el suficiente material de apoyo acorde a la capacitación, para ser proporcionados a los usuarios.

- Todas las capacitaciones deberán ser en ambientes de prueba.

- Para la realización de las capacitaciones antes deben hacerse revisiones de los activos informáticos y servicios relacionados con el tema.

- Es obligatorio que los funcionarios de la institución asistan a las capacitaciones.

9.1.3 Incidentes y atención a los usuarios

- Se generarán copias de respaldo o back-up para salvaguardar la información crítica en procesos institucionales significativos, estas deberán ser realizadas periódicamente en los equipos administrativos y servidores. Se realizara back-up registrando la fecha de copia, asunto, y se entregaran y almacenaran en las oficinas de la TICS.

- Es obligatorio reportar cualquier incidencia en cuanto a la seguridad informática a las TICS.

- Todas las solicitudes por parte de los funcionarios de la institución, serán gestionadas y solucionadas en el menor tiempo posible.

- Cada novedad reportada que se evalué como un riesgo en la seguridad de la información, se documentara detalladamente para ser analizada y crear controles para el aseguramiento de los activos de información.

9.1.4 Seguridad lógica.

- Se divide en: control de acceso, administración de acceso de usuarios, uso de contraseñas, responsabilidades de los usuarios y el uso del correo electrónico.

9.1.5 Control de acceso

- Es responsabilidad del grupo de la TICS, facilitar todos los documentos necesarios para el uso de los sistemas.

- La oficina de las TICS se encargara de notificar a todos los funcionarios nuevos de la institución en asignarle los roles correspondientes, los equipos, un usuario en la red y eliminación de éste.

- De acuerdo a sus roles en los sistemas de información que presenten los usuarios se definirán privilegios. Ya determinado, está prohibido intercambiar roles de las cuantas de acceso a los sistemas. Los responsables de velar por el cumplimiento será la oficina de las TICS.

- Para la solicitud de cualquier tipo de información deberá hacerse por escrito ante la dependencia responsable o de acuerdo a las políticas establecidas por la institución, de no cumplirse se procederá a:

- Canelar la solicitud presentada en su totalidad.

- Se procederá a denunciar a las autoridades competentes sobre el caso, una vez haya determinado el caso por el comité de seguridad informática.

9.1.6 Administración de acceso de usuarios

- Se llevara control a los accesos de los usuarios de la red institucional, entre estos están los administrativos, docentes, alumnos y cualquier persona que esté relacionada y haga uso de los servicios de la red.

- Para el acceso a los sistemas e información de la institución, el equipo de seguridad asignara a los usuarios una cuanta de acceso con previa clasificación y verificación de la función que desarrolla dentro de la institución.

- Todos los alumnos tendrán limitaciones en los accesos a la red, teniendo una red especial, donde gozaran de servicios de internet, en caso de alguna novedad o solicitud, deberá ser evaluada y si llegado el caso podrá ser modificado este control.

- Los usuarios de soporte técnico, los operarios, administradores de red, programadores de sistemas y administradores de bases de datos tendrán un identificador único para uso de personal exclusivo.

- Si los usuarios no cumplen con todos los requerimientos de autorización para algún tipo de servicio sin importar el área o dependencia o facultad, será denegado.

- La administración de las contraseñas serán implementadas por la oficina de las TICS, las cuales deberán cumplir los siguientes parámetros:

– Asignar contraseñas individuales para así determinar responsabilidades.

– El cambio de contraseña de los usuarios lo podrán realizar ellos mismos, de acuerdo a la selección establecida, se realizará de acuerdo al plan de mantenimiento establecido al cual se le establecerá un procedimiento de confirmación para contemplar los errores de ingreso.

– Las contraseñas establecidas, serán de calidad, según lo establecido en los procedimientos.

– Se registran las últimas contraseñas utilizadas por el usuario y así evitar la reutilización de las mismas.

– Es prohibido que las contraseñas se visualicen en pantalla, cuando son ingresadas.

– Los archivos de contraseña y los datos de sistemas de aplicación deberán ser almacenados en forma separada.

– Una vez instalados los componentes de software o hardware, las contraseñas que utiliza de forma predetermina, deberán ser modificadas.

9.1.7 Uso de contraseñas. Todas las contraseñas utilizadas por los usuarios, deberán cumplir los siguientes requisitos:

- Las contraseñas deberán tener una combinación alfanumérica.

- La longitud de las contraseñas deberán tener una longitud mínima de 10 caracteres.

- Las contraseñas no deberán utilizar datos personales, acrónimos o datos relacionados con el usuario.

9.1.8 Responsabilidades de los usuarios

- Los usuarios son responsables del uso que se le haga a la cuenta de acceso, equipos de cómputo y las contraseñas para el acceso a los sistemas.

- La contraseña proporcionada en medio digital o físico (documento o colilla) por el administrador de sistemas, deberá ser eliminada, con el propósito de evitar cualquier suplantación de identidad y mal uso de la información institucional como personal.

- En caso de no tener un sitio seguro para guardar la contraseña, se recomienda no hacerlo en agendas, papel o en un lugar de fácil acceso.

- La institución Luis Carlos Galán, no se hará responsable de la perdida información de los alumnos y personal en general.

- En caso de daño, falla, riesgo o amenaza detectada deberá ser reportada al responsable de las TICS, personal técnico o equipo de seguridad.

9.1.9 Uso del correo electrónico

- Los mensajes o archivos adjuntos, que se manejen dentro de la institución a los usuarios, serán de propiedad de la institución.

- Queda prohibido utilizar cuentas de correo electrónico que pertenezcan a otros usuarios, como también recibir mensajes en cuentas de otros, igualmente no se debe enviar correos con información institucional a correos externos de la institución, a menos con que cuente con autorización de la oficina de TICS.

- La información reservada o confidencial, que sea enviada por correo electrónico deberá ser encriptada y destinada exclusivamente a personas autorizadas en funciones institucionales.

10. ESTRATEGIAS DE DIVULGACIÓN DEL PROYECTO

El presente proyecto será divulgado y dado a conocer a toda la comunidad educativa de la Institución Educativa y Departamental Luis Carlos Galán del municipio de Yacopí Cundinamarca, como también a la Universidad Nacional Abierta y a Distancia UNAD, como requisito para obtener el título de especialista en informática, a través de las siguientes estrategias:

- Encuentros con docentes, estudiantes, administrativos y exalumnos por intermedio del equipo de gestión tecnológica y educativa, utilizando presentaciones didácticas.

- Se invitará a la comunidad en general y educativa, a visitar la página web de la institución[31], donde podrán encontrar toda la información suministrada en los encuentros realizados.

[31] COLEGIO DE TERAN. Nuestro colegio. [On line], [consultado el 2 de octubre de 2017]. Disponible en Internet: http://iedlcgyacopi.wix.com/iedlcgyacopi

11. CONCLUSIONES

Gracias al levantamiento de información llevado a cabo, se evidencia que la institución presenta un nivel de riesgo bastante alto, ya que la normatividad que presenta actualmente es muy vulnerable a ataques informáticos, pero con el apoyo de las directivas de la institución y todo el personal, se puede contrarrestar este tipo de situaciones.

Al implementar la metodología *Magerit* se logrará mitigar los riesgos que tiene la institución. Siendo una herramienta para reducir los riesgos, es de vital importancia mejorar las instalaciones alámbricas de red de la sede principal, teniendo en cuenta las normas internacionales, para la seguridad.

Se determinó que muchas de las fallas presentadas en el momento de registrar y almacenar la información sobre las calificaciones de los estudiantes en la plataforma *SIGES* se debió a la técnica de la ingeniería social.

Se establece de suma importancia realizar capacitaciones al personal, acerca de temas relacionados con la seguridad de la información, garantizando la concientización del valor de la información dentro de una organización, y que se tenga conocimiento de la posibilidad de ocurrencia de incidentes.

Además se establera políticas de seguridad en la institución, previniéndola de riesgos a los activos informáticos.

En el informe presentado a la institución se establecerá importante que las organizaciones inviertan en herramientas que permitan la gestión de redes, como también que se haga uso de herramientas de libre distribución, con el fin de obtener un valor agregado de seguridad en la organización; y que se haga énfasis en la concientización de seguridad tanto en niveles superiores de personal en una empresa, como en los demás empleados.

12. RECOMENDACIONES

Se debe identificar todos los activos de la institución, de esta manera poder brindar un grado de protección adecuada al activo más valioso de la institución que es la información, para ello se debe contratar personal competente en seguridad informática.

Se debe socializar y aprobar la ejecución de los controles propuestos al interior del I.E.D. Luis Carlos Galán.

Se deben realizar análisis periódicos de los riesgos, permitiendo analizar los riesgos; para de esta forma poder verificar y monitorear las acciones internas.

Las directivas administrativas deben de apoyar este estudio de seguridad informática y aplicarlo a la menor brevedad posible, y hacerle continuidad a este proyecto para el 2017.

Los usuarios y funcionarios de la institución deben recibir una capacitación y socialización del proyecto para poder aplicar las políticas de seguridad informática en pro de las mejores prácticas.

La metodología implementada debe ser utilizada exclusivamente para realizar auditorías de riesgos en el área informática ya que contiene actividades que puede ser aplicada en otras instituciones de nuestro medio.

Para una investigación a profundidad se debe realizar un estudio y análisis de metodologías existentes y se tomen en consideración, técnicas y herramientas de comparación avanzadas, que sea para aplicar las empresas de nuestro medio.

BIBLIOGRAFÍA

ADMINISTRACIÓN ELECTRÓNICA. ST 098 3/03/94: *Magerit* v3. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: http:// administracionelectronica.gob.es/pae_Home/ pae_ Documentacion/ pae_ Metodolog/pae_Magerit.html#.VCmVZhZRVJQ

BISOGNO, María Victoria Metodología para el aseguramiento de entornos informatizados – MAEI. Argentina: Universidad de Buenos Aires, 2004. [on line], [consultado el 3 de septiembre de 2017]. Disponible en internet: http://materias. fi.uba.ar/7500/bisogno-tesisdegradoingenieriainformatica.

BOLAÑOS, María C y ROCHA G. Mónica. 25 de marzo de 2014. Auditoria de SI. *MageritV3* (Metodología de Análisis y Gestion de Riesgos de los Sistemas de Información). [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: http://asijav.weebly.com/auditoria-de-sistemas-de-informacioacuten/magerit-v3-metodologa-eanlisis-y-gestin-de-riesgos-de-los-sistemas-de-informacion.

CANCELADO GONZÁLEZ, Alberto. El riesgo es una condición del mundo real en el cual hay una exposición a la adversidad. [on line], [consultado el 3 de septiembre de 2017]. Disponible en internet: stadium.unad.edu.co/preview/UNAD. php?url=/bitstream/ 10596/2655/3/76327474.

CERCA DE PIEDRA. ST- 02/92: Manual de convivencia. 2016. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: www.cercadepiedra.edu.co/ images/.../MANUAL_DE_ CONVIVENCIA_2016.

COLEGIO DE TERAN. Nuestro colegio. [On line], [consultado el 2 de octubre de 20017]. Disponible en Internet: http://iedlcgyacopi.wix.com/iedlcgyacopi

COLOMBIA. Corte Constitucional. ST 098 3/03/94: Nuevo Manual de Convivencia. 2015. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: manualmepalumnos. blogspot. com/2011/03/nuevo-manual-de-convivencia-2011.

_____. Sentencia T-**235/97**. Derecho a la educación. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: www.corteconstitucional.gov.co/ relatoria/1997/t-235-97.htm

_____. Sentencia No. T-**316/94**. Derecho a la educación/plantel educativo. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: www.corteconstitucional. gov.co/relatoria/1994/T-316-94.htm

_____. Sentencia T-397/97. Igualdad de derechos entre cónyuge y compañera permanente. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: www.corteconstitucional.gov.co/relatoria/1997/T-397-97.htm

_____. ST 439 12/10/94: falta de rendimiento académico. . [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: www.corteconstitucional. gov.co/relatoria/1997/T-397-97.htm

_____. Sentencia C-481/98. Régimen disciplinario para docente. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: www.corteconstitucional. gov.co/ relatoria/1998/c-481-98.htm

_____. Sentencia No. T-519/92. Derecho a la educación. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: www.corteconstitucional. relatoria/1992/T-519-92.htm

_____. T-527/95. Derecho a la educación. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: www.corteconstitucional. gov.co/relatoria/ 1995/t-527-95.htm

_____. ST 596 7/12/94: Sentencias y documentos de apoyo frente a las normas y manuales del colegio. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: https://www. facebook.com/notes/gestion comunitaria/3202324804

_____. T-612/92. Derecho a la educación. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: www.corteconstitucional.gov. co/ relatoria/ 1992/T-612-92.htm

_____. Principio de primacía de realidad sobre formalidades establecidas por sujetos de relaciones laborales/relación de trabajo

_____. Sentencia T-967 de 2007: Derecho a la educación frente a derechos económicos. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en internet: www.corteconstitucional. gov.co/relatoria/2007/t-967-07.htm

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Manual técnico del Modelo Estándar de Control Interno para el Estado Colombiano MECI 2014. Disponible en . p. 90

GALEANO VILLA, Jorge Luís y ÁLZATE CASTAÑEDA, Cristian Camilo. Protocolo de políticas de seguridad informática para las universidades de Risaralda. Pereira: Universidad Católica, 2013, p. 100

GOBIERNO DE ESPAÑA Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. 2012 *Magerit 3.0*. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: http://administracionelectronica.gob.es/

GONZÁLEZ BARROSO, Jesús. Catálogo de Elementos. Madrid. Ministerio de *Hacienda y Administraciones Públicas. (v.3.0): Metodología de análisis y Gestión de riesgos los sistemas de información.* Libro número II de la metodología *MAGERIT*, 2012 [on line], [consultado el 3 de septiembre de 2017]. Disponible en internet: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/ documentos/Documentacion/Metodologias-yguias/Mageritv3/2012_ Magerit_v3 _libro2_catalogo-de-elementos_ es_ NIPO_630-12-171-pdf

GUZMÁN GARCÍA, Alexánder y TABORDA BEDOYA, Carlos Alberto. Diseño de un sistema de gestión de la seguridad informática – SGSI–, para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C., a través de la auditoría, Bogotá, Colombia, Trabajo de grado (Especialización seguridad informática), Universidad Nacional Abierta y Distancia UNAD. Escuela de ciencias básicas tecnología e ingeniería. 2015, p. 311 disponible en el catálogo en línea de la Universidad UNAD. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en internet:: http://hdl.handle.net/10596/3448

INFOTEGRA.COM. (2017). *]macroproceso de apoyo proceso gestion apoyo academico.* [on line], [consultado el 3 de septiembre de 2017]. Disponible en internet: http://www.infotegra.com/ preview/UNAD.php?url=/bitstream/10596/pdf.

INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DEL CAUCA. Historia Institucional 1967-2011. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en internet: http://www.colmayorcauca.edu.co/unimayor/page/historia-institucional. Suministra información histórica y actual acerca del Colegio Mayor del Cauca.

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN (INTECO). Implantación de un SGSI en la empresa. . [on line], [consultado el 3 de septiembre de 2017]. Disponible en internet: http://cert.inteco.es/extfrontinteco/ img/File/ intecocert/sgsi/img/Guia_apoyo_SGSI.pdf.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 2700. Sistema de gestión de seguridad de la información. Términos de uso información. 2012. [on line], [consultado el 3 de septiembre de 2017]. Disponible en internet: www.iso27000.es/iso27000.html

ISACA Trust in, and value from, information systems. [On líne], [consultado el 2 de septiembre de 2017]. Disponible en internet: https://www.isaca.org/ Pages/ default.aspx

IZQUIERDO D, Fernando. La administración y los riesgos. [en line]. EN: Maxitana C, Jennifer D. (Auditor en control de gestión). Tesis: Administración de riesgos de tecnología de información de una empresa del sector informático. Guayaquil – Ecuador: Escuela Superior politécnica del Litoral, 2005. p.39. [on line], [consultado el 3 de septiembre de 2017]. Disponible en internet: http:// www.cib.espol.edu.ec/Digipath/D_Tesis_PDF/D-33960.pdf

MAGERIT V 3. (2010). *Catálogo de elementos.* . [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: https://es.scribd.com/document/.../MAGERIT-III-Libro-II-Catalogo-de-Elementos.

MINISTERIO DE EDUCACION NACIONAL. *Sistema de matriculas.* [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: http://www.sistema matriculas.gov.co/simat/app.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS TELECOMUNICACIONES. Ley 1273 de 2009. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-3705.html

PAREDES F. Geomayra y VEGA N. Mayra (2011). Desarrollo de una metodología para la auditoría de riesgos Informáticos (físicos y lógicos) y su aplicación al Departamento de informática de la dirección provisional de pichincha del consejo de la judicatura Escuela Superior Politécnica De Chimborazo 2011. Ecuador. [On line]: [consultado el 23 de septiembre de 2017]. Disponible en: http://dspace.espoch.edu.ec/bitstream/ 1234 56789/1497/1/18T00459.pdf

SECURITY JEIFER. ¿Qué es ciclo PHVA?. Enero 09 de 2010. Blog de seguridad informática. [on líne], [consultado el 2 de septiembre de 2017]. Disponible en internet: http://securityjeifer. wordpress.com/tag/phva/

SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ D.C. COMISIÓN DISTRITAL DE SISTEMAS. Resolución 305 de 2008 [on líne], [consultado el 2 de septiembre de 2017]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/ normas/Norma1. jsp?

SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ D.C. COMISIÓN DISTRITAL DE SISTEMAS. Décimo primer lineamiento inventarios de activos de información. Disponible en: <http://secretariageneralalcaldiamayor. gov.co/sites/files/lineamiento_11_inventario_de_activos_de_informacion.pdf>

SUAREZ, P. **Análisis y diseño de un sistema de gestión de seguridad informática.** 2013, p.45. [On line]: [consultado el 23 de septiembre de 2017].

Disponible en: stadium.unad. edu.co/ preview/ UNAD.php?url=/bitstream/10596/3777/1/2090454

SECUREIT. (2017). *Procesos y gobierno: anàlisis y gestión de riesgos.* [on líne], [consultado el 2 de septiembre de 2017]. Disponible en internet: https://www. secureit.es/procesos-y-gobierno-it/analisis-y-gestion-de-riesgos.

SIGES. (2017). *Sistema de Información para la gestión escolar.* [on líne], [consultado el 2 de septiembre de 2017]. Disponible en internet: http://se. cundinamarca.gov.co.6060/siges/.

VARGAS GUTIÉRREZ, Juan David. Tecnología en sistemas, diseño de un sistema de calificaciones WEB para el Colegio Alto Semisa. Puente Nacional (Santander): Universidad Abierta y a Distancia –UNAD- 2013, p. 108

VILCHES T, Martín. El riesgo [en line]. En: Machuca C, John. (Magister en Contabilidad y Auditoría). Tesis Guía para la evaluación del sistema de riesgo operativo en la Cooperativa de Ahorro y Crédito Jardín Azuayo. Cuenca – Ecuador. Universidad de Cuenca, 2011. p.21. [on line], [consultado el 3 de septiembre de 2017]. Disponible en internet: http://dspace.ucuenca.edu. ec/ bitstream/123456789/2729/1/tm4487.pdf

ANEXOS

ANEXO A. Clasificación de los activos

TIPO DE ACTIVO	DESCRIPCIÓN
[D] Datos / Información	Son elementos de hardware y software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional operativa y administrativa de cada entidad, órgano u organismo.[32]
[S] Servicios	Hace referencia a aquellas actividades realizadas por personas, dependencias o entidades ajenas al proceso, que facilitan la administración o flujo de la información generada por el proceso. En esta tipología se encuentra la intranet, el internet, el correo electrónico, el servicio de fotocopiado, el servicio de correspondencia, el servicio de ingreso a la entidad, entre otros[33].
[SW] Software / Aplicativos	Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora33. El Manual Técnico del MECI 2014 hace referencia a los programas, información y conocimiento (software) como "el conjunto ordenado de instrucciones, información y base de conocimientos dadas al computador y que son requeridas para el trabajo de estos sistemas"[34]

[32] SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ D.C. COMISIÓN DISTRITAL DE SISTEMAS. Resolución 305 de 2008 "por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre". Disponible en <http://www.alcaldiabogota.gov.co/sisjur/ normas/Norma1.jsp?i=33486>

[33]SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ D.C. COMISIÓN DISTRITAL DE SISTEMAS. Décimo primer lineamiento inventarios de activos de información. Disponible en: <http://secretariageneralalcaldiamayor.gov.co/sites/default/files/lineamiento_11_inventario_de_activos_de_informacion.pdf> p22

[34] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Manual técnico del Modelo Estándar de Control Interno para el Estado Colombiano MECI 2014. Disponible en . p. 90

ANEXO A…Clasificación de los activo (Continuación)

[HW] Equipamiento informáticos (Hardware)	El Manual Técnico del MECI 2014 hace referencia al Componente Físico (hardware) de los sistemas de información y comunicación como "el medio utilizado para realizar la captura, procesamiento, almacenamiento, difusión y divulgación de la información, es deseable que se utilicen las tecnologías de punta para lograr una gestión oportuna y eficiente en almacenaje y procesamiento de datos y en la ampliación de la cobertura de información a difundir"[35]
[COM] Redes de comunicaciones	Tiene que ver con todas las instalaciones utilizadas para las comunicaciones dentro de la institución, transportando datos de un lado a otro.
[Media] Soportes de información	Son los dispositivos físicos utilizados para el almacenamiento de información. Ejemplo: memorias USB, CD-ROM, material impreso.
[AUX] Equipamiento auxiliar	Son los dispositivos que complementan los sistemas de información como son UPS, cableado, aires acondicionados, entre otros.
[L] Instalaciones	Cableado estructurado, instalaciones eléctricas, relacionados con los sistemas de información y comunicaciones.
[P] Personal	Se relaciona a todo el personal que se encuentre relacionado con los sistemas de información de la institución, tanto personal interno como externo.
[SI] Sistema de Información	Son ficheros, bases de datos, documentos de sistemas, materia de información, aplicaciones de sistemas, equipos informáticos entre otros.

[35] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Manual técnico del Modelo Estándar de Control Interno para el Estado Colombiano MECI 2014. Disponible en . p. 90

ANEXO B. Encuesta aplicada

A continuación se anexa la encuesta realizada a 20 usuarios de la institución.

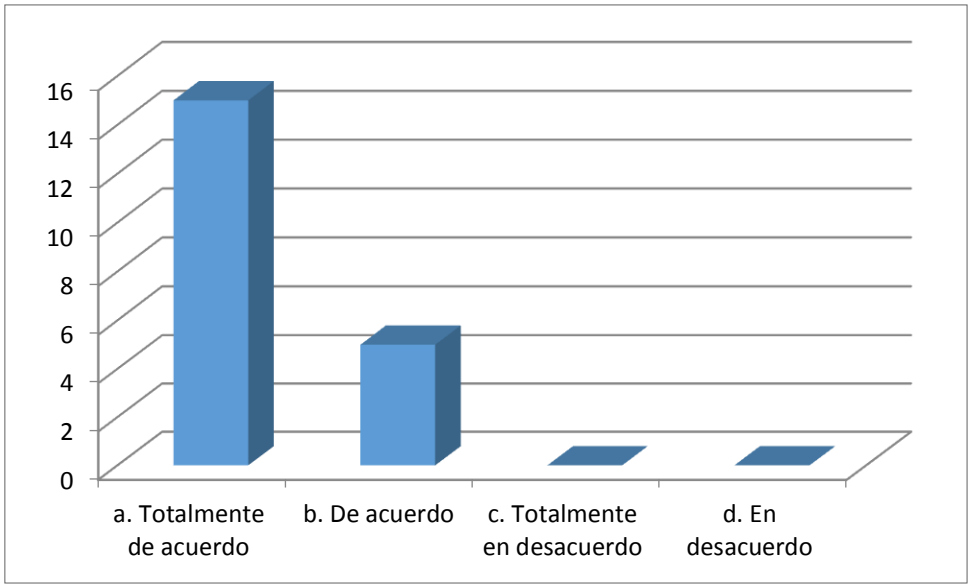
<table>
<tr><th colspan="2">INSTITUCIÓN EDUCATIVA DEPARTAMENTAL LUIS CARLOS GALÁN</th></tr>
<tr><td colspan="2">Reciban un cordial saludo estamos interesados en conocer su opinión como miembro de la comunidad educativa de la I.E.D. Luis Carlos Galán, por favor ¿sería tan amable de contestar el siguiente cuestionario? La información que nos proporcione será utilizada para conocer la viabilidad de desarrollar políticas de seguridad de la información para la institución. Gracias.</td></tr>
<tr><td>1. ¿Es importante el registro y control de la información confidencial de la institución en base a políticas para la seguridad de la información?
a. Totalmente de acuerdo
b. De acuerdo
c. Totalmente en desacuerdo
d. En desacuerdo</td><td>3. ¿Considera que el control de acceso para personal ajeno a la institución cumple con las normas mínimas de seguridad de la información confidencial?
a. Si
b. No</td></tr>
<tr><td>2. ¿Cuál de las siguientes características considera importante para el control en el manejo de la información?
a. Tener ciertas restricciones como ente gubernamental, utilizando contraseñas personalizadas para el uso de los equipos de cómputo.
b. Prohibirse el acceso a páginas web no autorizadas por la institución.
c. Tener definido un Sistema de Gestión de la Seguridad de la Información con sus políticas definidas y debidamente controladas.
d. Todas las anteriores.</td><td>4. De las siguientes anomalías seleccione aquellas con respecto a la seguridad informática de la información.
a. Se ha presentado la perdida de información importante en memorias USB.
b. El funcionario asegura haber dejado el equipo apagado y lo encuentra encendido con su usuario abierto.
c. Se ha presentado daños en la información por ataques de virus injustificados.
d. El personal permanece mucho tiempo en sitios web no permitidos.</td></tr>
</table>

A continuación se representan las tablas y gráficos que corresponde a la información recolectada de la encuesta realizada.

1. ¿Es importante el registro y control de la información confidencial de la institución en base a políticas para la seguridad de la información?

Tabla 29. : Pregunta 1 encuesta

RESPUESTA	TOTAL
	CANTIDAD
a. Totalmente de acuerdo	15
b. De acuerdo	5
c. Totalmente en desacuerdo	0
d. En desacuerdo	0
TOTAL	20



Fuente: autor

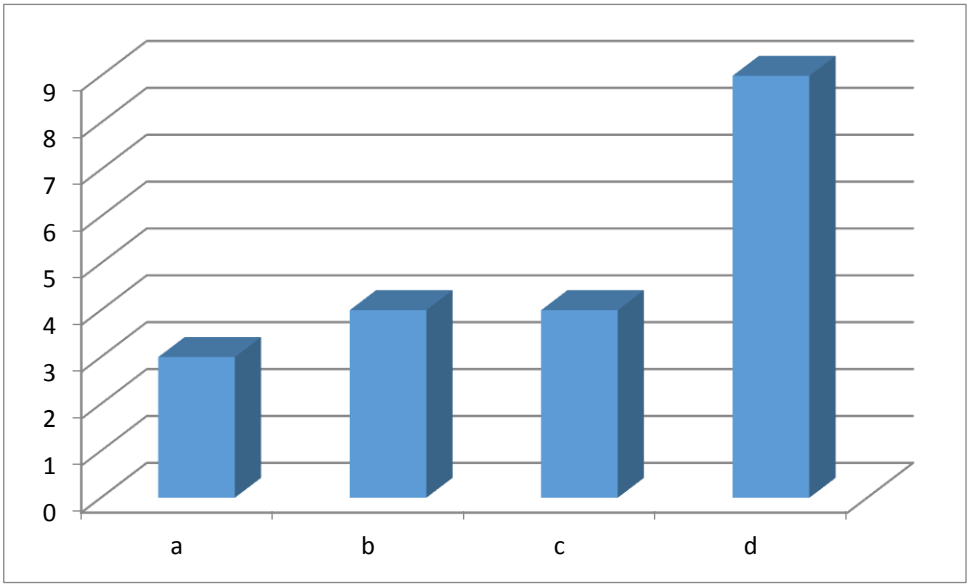
Interpretación:

De 20 usuarios y funcionarios encuetados, el 75% estuvieron totalmente de acurdo con la implementación del control y registro de la información dentro de la institución y un 15% de acuerdo.

2. ¿Cuál de las siguientes características considera importante para el control en el manejo de la información?

Tabla 30: Pregunta 2 encuesta

RESPUESTA	TOTAL CANTIDAD
a. Tener ciertas restricciones como ente gubernamental, utilizando contraseñas personalizadas para el uso de los equipos de cómputo.	3
b. Prohibirse el acceso a páginas web no autorizadas por la institución.	4
c. Tener definido un Sistema de Gestión de la Seguridad de la Información con sus políticas definidas y debidamente controladas.	4
d. Todas las anteriores.	9
TOTAL	20



Fuente: autor

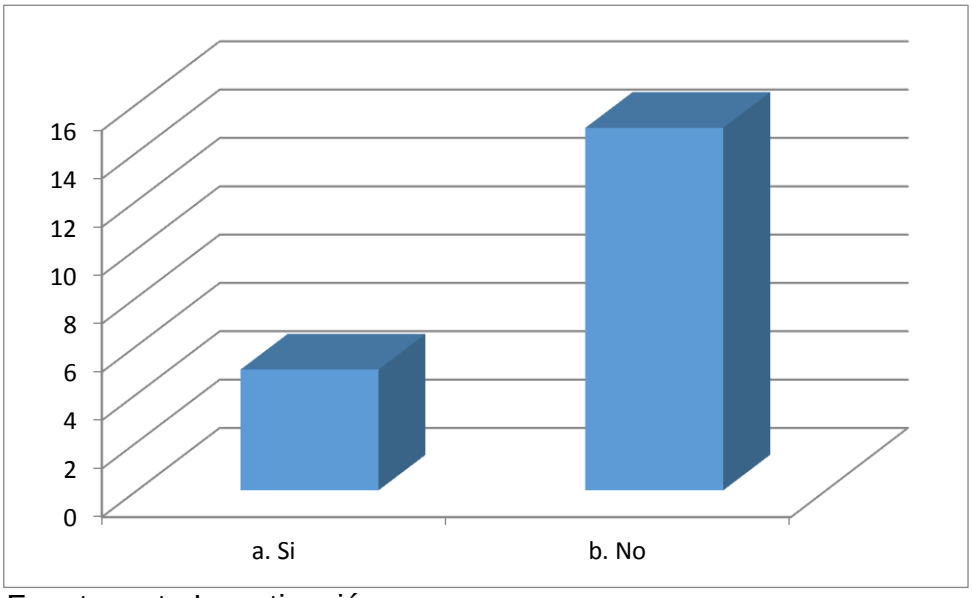
Interpretación:

El 45% de los encuestados considera que es importante el control y manejo de la información y declarando que todas las normas de control son importantes para la institución.

3. ¿Considera que el control de acceso para personal ajeno a la institución cumple con las normas mínimas de seguridad de la información confidencial?

Tabla 31: Pregunta 3 encuesta

RESPUESTA	TOTAL
	CANTIDAD
a. Si	5
b. No	15
TOTAL	20



Fuente: esta Investigación

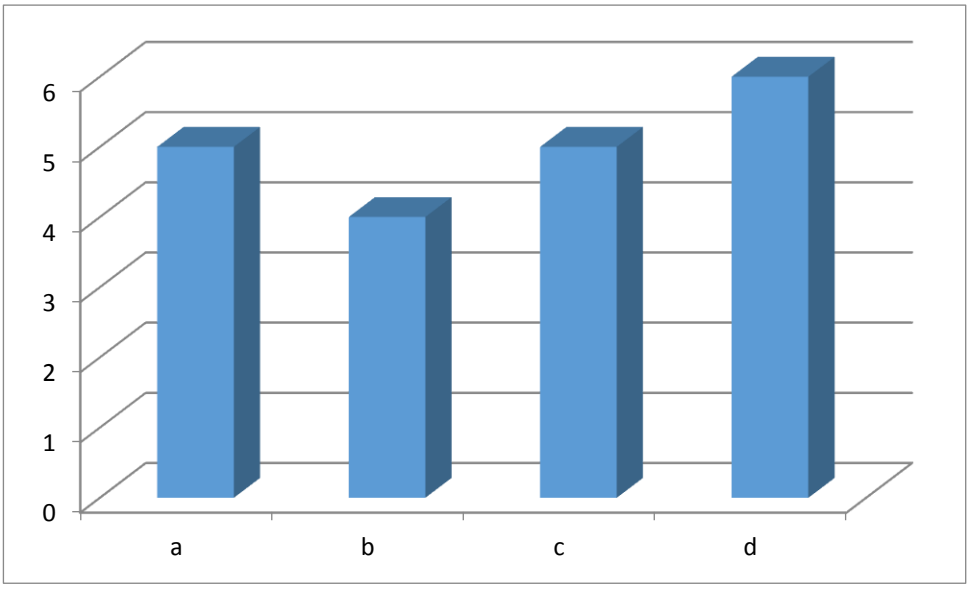
Interpretación:

El 75% de los encuestados considera que las normas mínimas de seguridad implementadas dentro de la institución no cumplen con la protección adecuada de la información, siendo estas muy vulnerables.

4. De las siguientes anomalías seleccione aquellas con respecto a la seguridad informática de la información.

Tabla 32: Pregunta 4 encuesta

RESPUESTA	TOTAL
	CANTIDAD
a. Se ha presentado la perdida de información importante en memorias USB.	5
b. El funcionario asegura haber dejado el equipo apagado y lo encuentra encendido con su usuario abierto.	4
c. Se ha presentado daños en la información por ataques de virus injustificados.	5
d. El personal permanece mucho tiempo en sitios web no permitidos.	6
TOTAL	20



Fuente: autor

Interpretación:

Nos damos cuenta que existen diferentes tipos de vulnerabilidades dentro del sistema de seguridad de la información, ya que no existe unas normas claras durante la implementación de éstas.

ANEXO C. Autorización auditoria institución

Institución Educativa Departamental Luis Carlos Galán Municipio de Yacopí
Resolución de Aprobación Nº 007809 de 06 Dic 2010
DANE: *225885002031* CÓDIGO ICFES: 132514 NIT: *900008138-9*

Yacopí, noviembre 6 de 2017

Señor
JOSÉ EDWIN GONZÁLEZ RETAMOZO
Ing. Informático
Docente
Institución Educativa Luis Carlos Galán

REF. APROBACIÓN AUDITORIA DE SEGURIDAD INFORMÁTICA PARA LA INSTITUCIÓN EDUCATIVA DEPARTAMENTAL LUIS CARLOS.

De acuerdo a su solicitud expresada, es muy grato comunicarle a usted, ***José Edwin González R.*** docente de la institución y estudiante de la especialización en Seguridad Informática de la universidad UNAD. Darle el visto bueno para llevar a cabo su proyecto de auditoria en seguridad informática como requisito para su graduación en dicha especialización.

Esta auditoria tiene como objetivo llevar una evaluación crítica al área informática mediante técnicas y procedimientos que permitan constatar si las actividades de los sistemas son correctas y están de acuerdo con las normativas informáticas y generales de la institución y dar sugerencias a las soluciones estratégicas a los hallazgos.

Cabe mencionar que toda aquella información recopilada por la auditoria propuesta, será considerada de reserva profesional y conocidas por las contrapartes.

Atentamente.

Pedro Eliberto Quiroga R.

PEDRO ELIBERTO QUIROGA RUEDA
RECTOR

Inspección de Terán Yacopí, Cundinamarca – email: iedteran@hotmail.com
Página Web: iedlcgyacopi.wixsite.com/iedlcgyacopi
Celular: 321 222 9789 – 312 866 2915 – 313 825 4665