DISEÑAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL COLEGIO AGROINDUSTRIAL DE PUERTO NUEVO DEL MUNICIPIO DE SIMACOTA (SANTANDER), BASADO EN LA NORMA 27001: 2013

ING. ALIX RUEDA LEON COD: 37.652.423

ING. JOSE DARLING CASTILLO SARMIENTO COD: 88.141.638

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESPECIALIZACION EN SEGURIDAD INFORMATICA

BUCARAMANGA

2017

DISEÑAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL COLEGIO AGROINDUSTRIAL DE PUERTO NUEVO DEL MUNICIPIO DE SIMACOTA (SANTANDER), BASADO EN LA NORMA 27001: 2013

ING. ALIX RUEDA LEON COD: 37.652.423 GRUPO 16

ING. JOSE DARLING CASTILLO SARMIENTO COD: 88.141.638

MAG. GABRIEL MAURICIO RAMIREZ

Proyecto aplicado para optar a titulo

de Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESPECIALIZACION EN SEGURIDAD INFORMATICA

BUCARAMANGA

2017

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bucaramanga , 02 de Noviembre de 2017

DEDICATORIA

A Dios por haberme permitido llegar a este momento tan especial en mi existencia, dandome salud para lograr mis objetivos; por los triunfos y momentos dificiles que me han enseñado a valorar cada instante de la vida y por su infinita bondad y amor que permite tener todo según sea su voluntad.

A mis padres, por ser una fuente constante de inspiración no hay un día en el que no le agradezca a Dios haberme colocado entre ustedes; la fortuna más grande es tenerlos conmigo y el tesoro más valioso son todos y cada uno de los valores que me inculcaron. A mi esposo Jorge Leonardo por ser el apoyo, la motivación constante, por su amor y porque en el recorrer de nuestro camino siempre ha sido el motor para salir adelante.

A mi señora esposa Celeida Montaño Meneses y mi hija Marian Alexandra, incondicionales con su apoyo en algunos de los momentos màs críticos de mi vida, brindandome su amor para lograr los objetivos cumplidos. A mis hermanas: Ingrid, Lizbeth, Alma, Sandra y Rocio Castillo Sarmiento, a cada una de ustedes les agradezco por sus innumerables consejos.

CONTENIDO

Pág.

INTRODUCCION 12

1. DEFINICION DEL PROBLEMA 13

1.1.FORMULACION DEL PROBLEMA 15

2. JUSTIFICACION 16

3. OBJETIVOS 18

3.1.OBJETIVO GENERAL 18

3.2.OBJETIVOS ESPECIFICOS 18

4. MARCO REFRENCIAL 19

4.1.MARCO TEORICO 19

4.1.1. Norma ISO 27001 19

4.1.2. Herramientas aplicables al Sistema general de Seguridad de la Información 20

4.2.MARCO CONCEPTUAL 21

4.3.ANTECEDENTES 24

4.4. MARCO CONTEXTUAL 27

4.4.1. Reseña histórica 27

4.4.2. Misión 28

4.4.3. Visión 28

4.4.4. Políticas administrativas 28

4.4.5. Organigrama Institucional 29

4.4.6. Permisos 29

4.5. MARCO LEGAL 29

4.5.1. Ley 603 del 2000 29

4.5.2. Ley estatutaria 1266 de 2008 30

4.5.3. Ley 1273 de 2009 30

4.5.4. Ley 1341 de 2009 30

4.5.5. Ley estatutaria 1581 de 2012 31

5. DISEÑO METODOLOGICO 32

5.1. Metodología de la investigación 32

5.2. Enfoque de investigación 32

5.3. Tipo de Investigación 32

5.4. Instrumentos de recolección de información 33

5.5. Población y muestra 33

5.5.1. Población 33

5.5.2. Muestra 34

5.6. Metodología de desarrollo 36
5.6.1. Primera fase 36
5.6.2. Segunda fase 36
5.6.3. Tercera fase 36
5.6.4. Cuarta fase 37

6. DESARROLLO DEL PROYECTO 38
6.1. Planificación del proyecto 38
6.2. Análisis de resultados 39
6.2.1. Análisis de la observación directa 39
6.3. Análisis y evaluación de riesgos de los activos de información 46
6.3.1. Tipos de Activos 47
6.3.2. Vulnerabilidades, Amenazas y riesgos de seguridad del área informática 47
6.4. Evaluación de nivel del Impacto 48
6.4.1. Resultado Evaluación del nivel de Impacto 49
6.5. Implementación de Salvaguardas 49
6.5.1. Salvaguardas 50
6.6. Políticas de Seguridad 51

7. RECURSOS NECESARIOS PARA EL DESARROLLO DEL PROYECTO 54

8. CRONOGRAMA DE ACTIVIDADES 55

9. CONCLUSIONES 56

BILIOGRAFIA 58

ANEXOS 59
ANEXO A Carta de Aceptación 59
ANEXO B Tipos de Activos 60
ANEXO C Vulnerabilidades, amenazas y riesgos de seguridad del área informática 64
ANEXO D Resultado Evaluación del nivel de impacto 67
ANEXO E Salvaguardas 72

LISTA DE TABLAS

Pág.

Tabla 1. Activos informáticos 35

Tabla 2. Inventario de Activos 47

Tabla 3. Vulnerabilidades, amenazas y riesgos de seguridad 47

Tabla 4. Escala de Rango de frecuencia de amenazas 48

Tabla 5. Dimensiones de seguridad 48

Tabla 6. Escala de Rango porcentual de impactos en los activos para cada dimensión de seguridad. 49

Tabla 7. Efectos y tipo de salvaguardas 49

Tabla 8. Salvaguardas de Soportes de Información almacenamiento Electrónico 50

Tabla 9. Presupuesto 54

Tabla 10. Cronograma de actividades 55

GLOSARIO

SGSI: Sistema de Gestión de la Seguridad de la Información, es, como el nombre lo sugiere, un conjunto de políticas de administración de la información[1].

ACTIVOS: Según define el Marco conceptual del Plan General de Contabilidad español, los activos son los bienes, derechos y otros recursos controlados económicamente por la empresa, resultantes de sucesos pasados de los que se espera obtener beneficios o rendimientos económicos en el futuro.

INFORMACIÓN: Está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

AMENAZAS: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.

RIESGOS: Es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

METODOLOGÍA MAGERIT 3.0: Es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno.[2]

POLÍTICAS: Una política de seguridad es un conjunto de reglas y prácticas que regulan la manera en que se deben dirigir, proteger y distribuir los recursos en una organización para llevar a cabo los objetivos de seguridad informática de la misma.

---

[1] El portal de ISO 27002 en Español. Políticas de Seguridad. Revisado en: http://www.iso27000.es/iso27002_5.html

[2] MAGERIT 3.0. Metodología de Análisis y Gestión de Riesgos de los sistemas de Información. Libro 1. Madrid. Octubre de 2012.

RESUMEN

Este trabajo está orientado al diseño del Sistema de Gestión de Seguridad de la Información para el Colegio Agroindustrial de Puerto Nuevo del municipio de Simacota (Santander), con el único propósito de asegurar los activos de información de dicha entidad, se recogen aspectos muy importantes iniciando con un recorrido por la institución conociendo su planta física, los servicios que ofrece, entrevistando a la rectora, secretario y docentes sobre la información que se maneja, analizando las posibles vulnerabilidades y los riesgos existentes, con la intención de identificar los riesgos y amenazas de los activos vinculados.

Con la recolección de información se inicia el proceso de diseño del SGSI identificando los riesgos y amenazas, estableciendo los controles para salvaguardar la información, realizando el proceso de verificación a cada activo de la institución, esto con el visto bueno de las directivas y demás personal con el fin de ir familiarizando en el tema.

Además se le entregan formatos para dar inicio al seguimiento del SGSI, para llevar los controles en orden y en el momento de realizar las auditorias tener los entregables sin ninguna objeción, creando políticas a cada activo encontrado según los riesgos analizados y categorizados en la metodología *Magerit* 3.0.

Palabras claves: SGSI, ACTIVOS, INFORMACIÓN, AMENAZAS, RIESGOS, METODOLOGÍA MAGERIT 3.0, POLÍTICAS.

INTRODUCCIÓN

Actualmente el diseño del Sistema de Gestión de Seguridad de la Información ya es una necesidad en las instituciones tanto públicas como privadas, en pequeñas, medianas y grandes empresas; porque los administradores ya tomaron conciencia que el activo más valioso de una empresa es la información. Cuando se habla de información se abarca todo lo que puede ser tanto físico como medio magnético entre ellos archivos, carpetas, documentos, y demás que pueden estar interna o externamente en la institución.

Para el lugar de estudio que es el Colegio Agroindustrial de Puerto Nuevo, esta institución maneja información importante porque almacena datos personales de estudiantes, padres de familia, docentes y directivos y no tiene control para asegurar y garantizar la confidencialidad, integridad, y disponibilidad del sistema documental de la información del colegio; además están a la orden de perdida de información por motivos de desastres naturales, robo de información, acceso abusivo y entre otros que evidencia la necesidad de diseñar el sistema de gestión de seguridad de la institución nombrada para tomar medidas de prevención y control a estas falencias.

Por lo tanto el objetivo del desarrollo de este trabajo es diseñar el sistema general de seguridad de la información en la institución, involucrando a toda la comunidad educativa para que tome conciencia de la necesidad de resguardar y organizar la información digital, identificando los riesgos existentes y las vulnerabilidades encontradas con el fin de que hagan uso de los controles, normas y políticas de seguridad que dan solución a la problemática, educándolos en el manejo de las TIC y el uso de buenas prácticas.

De manera que en el siguiente documento se encontrara el resultado del estudio de una problemática presentada en el Colegio Agroindustrial de Puerto Nuevo, en el cual se evaluarán los riesgos, vulnerabilidades y amenazas de los activos y recursos de la institución, las posibles salvaguardas y las políticas de seguridad para mitigar el impacto y reducir o eliminar el riesgo.

1. DEFINICION DEL PROBLEMA

El Colegio Agroindustrial de Puerto Nuevo se encuentra ubicado en el municipio de Simacota departamento de Santander. Actualmente tiene en su sede principal ciento noventa y cinco (195) alumnos y seis (6) sedes de primaria con doscientos (200) estudiantes, ofreciendo sus servicios un total de trescientos noventa y cinco (395) alumnos desde los niveles de jardín a undécimo grado, para lo cual posee una planta de veintitrés (23) profesores en todas las áreas de aprendizaje. [3]

Hoy en día la tecnología es un tema que avanza a pasos agigantados, puesto que con ella llegan los diferentes tipos de ayuda para hacer mejor las cosas, y por lo tanto se deben afrontar cambios importantes en la infraestructura tecnológica y sistematización de los procesos; ya que también todo tipo de innovación trae consigo amenazas y vulnerabilidades, que pueden ser aprovechadas por los expertos en el tema para acceder a la información, secuestrando o robándola; generando con ello problemas relacionados con la seguridad de la información.

Con base en lo anterior, en Colombia fue aprobada la norma ISO 27001:2013 a través del CONPES 3854 de 2016[4], la cual consiste en modernizar y aprender a reaccionar ante los riesgos de posibles peligros, en cuanto a infraestructura e información digital, por lo que el gobierno nacional invirtió alrededor de 85.070 millones de pesos para ejecutar entre el periodo comprendido entre los años 2016 y 2019. [5]

El principal objetivo de la norma ISO 27001 es identificar, gestionar y mitigar riesgos basados en procesos, ya que evalúa y controla a la organización en relación a los riesgos que presenta y está sometido el sistema de información. Por tanto con la implementación de esta norma las organizaciones pueden lograr una ventaja competitiva.[6]

---

[3] Portafolio educativo. Información suministrada por secretaría.

[4] DEPARTAMENTO NACIONAL DE PLANEACIÓN. (2016). Documento CONPES 3854. Bogotá, D.C.: Autor

[5] Para el país, la seguridad digital es una política nacional. Revisado en: http://www.portafolio.co

[6] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma Técnica Colombiana: NTC-ISO-IEC 27001. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Bogotá: ICONTEC. 2013.

El Colegio carece de manuales de procesos, lineamientos generales y objetivos claros, repercutiendo en la falta de conocimiento de los deberes y derechos de sus trabajadores. Así mismo, no cuenta con sistemas de información ágiles y oportunos, puesto que poseen la documentación administrativa solo en archivos físicos, dificultando en muchos casos la búsqueda y reporte de la misma. Por ende, los procesos no son estandarizados, documentados ni caracterizados, ya que carecen de indicadores de gestión para el seguimiento y medición del desempeño.[7]

Los inconvenientes encontrados se presentan así[8]: la documentación no cuenta con procedimientos normalizados, los procesos y su metodología se encuentran en la memoria de los trabajadores del plantel, lo que genera alta dependencia y pérdidas recurrentes de información. Puesto que no existen procesos informáticos que ayuden a mantener actualizados este tipo de proceso o archivos de texto, facilitando a los educadores en la ejecución de los mismos.

El Colegio carece de herramientas de medición, lo cual hace subjetivo el desempeño de los procesos y dificulta la toma de decisiones asertivas; ya o que al no contar con herramientas de almacenamiento de información dificulta estos procesos. El enfoque en objetivos no se con una estrategia organizacional definida, la visión, misión y objetivos se encuentran en proceso de construcción, dificultando que el personal tenga claridad sobre el desarrollo de planes estratégicos y tácitos para alcanzar los objetivos de la institución.

Y el grado de Satisfacción**.** No se tienen mediciones soportadas sobre la satisfacción de los estudiantes, docentes, administrativos, padres de familia y demás usuarios, por ende no se generan acciones que conlleven al mejoramiento de sus procesos internos y el establecimiento de herramientas tecnológicas permanentes, que ayuden a mantener este factor de comportamiento constante para saber el grado de satisfacción.

De acuerdo con lo anterior, la Institución Educativa debe considerar la implementación del Sistema de Gestión de Seguridad de la Información y el establecimiento de una política de seguridad de la misma, debidamente difundida y documentada; con el propósito de evitar la exposición de riesgos continuos que pueden incidir en la pérdida o alteración de los datos, y la definición de controles para la gestión de activos de la información. Ya que al no tener establecido dicho sistema de gestión, generará riesgos y amenazas que pueden impactar negativamente el desarrollo de los procesos institucionales.

---

[7] Información recolectada en la visita que se hace al colegio

[8] Ibíd.

1.1. FORMULACIÓN DEL PROBLEMA

¿Con el diseño de un sistema de seguridad de la información y políticas de seguridad para el Colegio Agroindustrial de Puerto Nuevo se podrá minimizar, salvaguardar y proteger la información de ataques informativos; garantizando y asegurando la confidencialidad y disponibilidad de esta en el momento que sea requerida?

2. JUSTIFICACIÓN

En la actualidad toda organización sin importar su tamaño o tipo; procesan, archivan y transmiten información sobre su accionar por medio de los diferentes elementos de almacenamiento de datos; razón por la cual es necesario que desde los procesos de operaciones hasta las políticas de uso de recursos, sean definidos a un nivel general, de manera confiable.

Si bien gran parte de la información se vincula con computadoras y redes, hay otra parte que no se representa en forma de bits, sino por ejemplo en papeles, en la memoria de las personas, en el conocimiento y experiencia de la organización misma, en la madurez de sus procesos, etc. En ambos casos, la información debe ser protegida de manera diferente, por lo que se hace necesario los Sistemas de Gestión de la Seguridad de la Información (SGSI).[9]

Con base en lo anterior, este diseño es necesario realizarlo en el Colegio Agroindustrial de Puerto Nuevo Santander, ya que no cuenta con un sistema que pueda asegurar y garantizar la confidencialidad, la integridad y la disponibilidad de la información, por tanto el activo más valioso de la población estudio se encuentra desamparado a la disposición de cualquier amenaza, tanto interna como externa. [10]

Es así que al diseñar el SGSI para la Institución Educativa, se tendrá resguardada y organizada la información digital que se maneja tanto en el área administrativa como en la académica. Puesto que en la visita realizada al Colegio, se observó que la información de los estudiantes, docentes, padres de familia y demás involucrados en esta organización, se encuentra almacenada en carpetas dentro de cajas de cartón, expuestas al deterioro por el polvo y el moho, a desastres naturales como incendios e inundaciones y al robo de la información por estar a la mano de todos. [11]

Igualmente, en las áreas administrativa y académica se maneja toda clase de información como los datos personales de padres de familia y alumnos, notas, horarios académicos, hojas de vida de los docentes y administrativos, planes de área, contratos y demás documentos que reposan en el archivo físico existente; los cuales merecen contar con las políticas mínimas de seguridad como disponibilidad, desempeño, confidencialidad, integridad y control de acceso físico y

---

[9] PACHECO, Federico, La importancia de un SGSI {En línea}. 03 octubre de 2017. Disponible en: (http://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/)

[10] Sistema de Gestión de la Seguridad de la Información. Procedimientos de Seguridad de la información. MINTIC. Revisado en: http://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

[11] Información recolectada en la visita que se hace al colegio.

lógico a la información manteniendo de ello copias de seguridad actualizadas periódicamente. [12]

De manera que al diseñar el SGSI se cumplirá con asegurar y garantizar la confidencialidad, la integridad y la disponibilidad de la información cumpliendo de esta manera con el objetivo del Sistema de Gestión de Seguridad de la Información, y por lo tanto minimizando las vulnerabilidades detectadas en el momento del estudio de la problemática.

Así mismo, el SGSI además de proteger los activos informáticos e información vulnerable, permitirá según lo establecido en la Norma ISO 27001:2013 emplear practicas apropiadas de seguridad de la información, concientizando a todos los miembros del Colegio sobre los riesgos y amenazas actuales; puesto que con la aplicación de una Política de Seguridad de la Información se creará en todos los integrantes de la Institución una cultura de seguridad que propenda por salvaguardar de ataques informáticos la documentación institucional.

[12] ISO 27000.ES. "El Portal de ISO 27001 en Español". {En línea}. {5 de mayo de 2017}. Disponible en: (http://www.iso27000.es/herramientas.html).

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información para el Colegio Agroindustrial de Puerto Nuevo del municipio de Simacota (Santander), basado en los requisitos de la norma 27001: 2013, que permita asegurar y garantizar la confidencialidad, integridad, y disponibilidad de la información.

3.2. OBJETIVOS ESPECÍFICOS

- Realizar un análisis de la situación actual de la Institución Educativa de Puerto Nuevo, acorde a los requerimientos de la Norma ISO 27001:2013

- Evaluar los riesgos, vulnerabilidades y amenazas encontradas en los activos y recursos de la Institución y el nivel de impacto de cada uno de ellos, y la implementación de salvaguardas con el fin de lograr la reducción o eliminación total de los riesgos informáticos.

- Definir las políticas de seguridad de la información que estén acorde con los lineamientos, procesos y requerimientos institucionales.

- Presentar ante el Consejo Directivo del Colegio Agroindustrial de Puerto Nuevo el diseño del Sistema de Gestión de Seguridad de la información basado en la Norma ISO 27001:2013

4. MARCO REFERENCIAL

4.1. MARCO TEORICO

4.1.1. Norma ISO 27001

Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos; puesto que proporciona la solución de una mejora continua para evaluar los diferentes riesgos y establecer las diferentes estrategias y controles para asegurar la protección y defensa de la información. [13]

Por lo tanto, los Sistemas de Gestión de la Seguridad de la Información (SGSI12) provee un modelo para establecer, implementar, monitorear, revisar, mantener y mejorar la protección de los activos informáticos para lograr los objetivos organizacionales basados en una gestión del riesgo y en los niveles aceptables de riesgos diseñados efectivamente para tratarlos y gestionarlos, analizando los requerimientos para la protección de los activos informáticos y aplicando los controles apropiados para asegurar que la protección de éstos activos contribuyen a la implementación exitosa del mismo.[14]

La norma ISO27001, Sistema de Gestión de Seguridad de la Información, es la solución de mejora continua más apropiada para poder evaluar los diferentes

---

[13] ISO 27000.ES. "El Portal de ISO 27001 en Español". {En línea}. {5 de mayo de 2017}. Disponible en: (http://www.iso27000.es/herramientas.html).

[14] ISO/IEC. International Standard ISO/IEC 27000: Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary. Geneva: ISO Copyright Office. 2014. p. 13.

riesgos y establecer una serie de estrategias y controles oportunos para asegurar la protección y defender la información; la cual utiliza el enfoque basado en procesos que usan el ciclo de Deming o el ciclo de mejora continua, consistente en Planificar-Hacer-Verificar-Actuar (PHVA), conocido con las siglas en inglés PDCA. [15] Este modelo consta de las siguientes fases que permiten medir el estado actual del sistema, con el fin de realizar un mejoramiento continuo:

Planear (Plan): En esta fase se diseña o planea el SGSI, definiendo las políticas de seguridad generales que aplicarán a la organización, los objetivos que se pretenden y cómo ayudarán a lograr los objetivos misionales; de igual manera se realiza el inventario de activos y la selección de la metodología de riesgos a implementar, los cuales deben estar acordes a los objetivos y políticas propuestos.

Hacer (Do): Es la fase donde se implementa el SGSI mediante la aplicación de los controles de seguridad escogidos, asignado los responsables y la ejecución de los procedimientos.

Verificar (Check): Es la fase de monitorización del SGSI donde se verifica y audita que los controles, políticas, procedimientos de seguridad se están aplicando de la manera esperada.

Actuar (Act): Esta fase implementa las acciones correctivas y mejoras del SGSI

De acuerdo con lo anterior, la aplicación de la Norma ISO 27001-2013 propende por la protección de la confidencialidad, integridad y disponibilidad de la información del Colegio Agroindustrial de Puerto Nuevo; a través de la identificación de los diferentes riesgos que pueden afectar la información y el diseño de los mecanismos óptimos para impedir o mitigar sistemáticamente el impacto de los mismos.

4.1.2. Herramientas aplicables al Sistema General de Seguridad de la Información

La principal referencia bibliográfica para la implementación del Sistema General de Seguridad de la Información es la norma ISO/IEC 27001 versión 2013, que contiene los lineamientos necesarios para implementar el SGSI; de igual manera se encuentra la Norma Técnica Colombiana NTC-ISO/IEC 27001 del año 2006, la cual es adaptada a procesos en Colombia por ICONTEC.

[15] GÓMEZ, L., ANDRÉS, A. Guía de Aplicación de la Norma UNE-ISOG/IEC 27001 Sobre Seguridad en Sistemas de Información para PYMES. España: Asociación Española de Normalización y Certificación. 2012.

Así mismo, existe el Manual de Metodología Abierta de Testeo de Seguridad (OSSTMM), el cual es uno de los estándares profesionales más completos y utilizados en auditorías de seguridad; y tiene como propósito realizar la revisión de la seguridad de los sistemas desde internet, incluye un marco de trabajo aplicable con las fases que se deben hacer para la ejecución de la auditoría.

Con el sistema operativo KaliLinux se puede realizar las pruebas de intrusión con las herramientas que tiene incorporado dicho sistema; con este se pueden hacer pruebas Testing a las bases de datos, páginas web, redes y sistemas operativos. Igualmente, el Ministerio de Tecnologías de la Información y las Telecomunicaciones en Colombia cuenta con un grupo de expertos parar crear modelos de seguridad a las entidades del Estado, los cuales sirven de guías para el diseño de sistemas de gestión de seguridad, puesto que ofrecen los lineamientos que se deben cumplir para lograr este objetivo.[16]

En Colombia existen algunas normas que sirven de apoyo en la parte de seguridad informática como son: la sentencia C-662 de la Corte Constitucional del 8 de Junio de 2000 sobre Mensajes de datos, Comercio Electrónico y Firma Digital; Ley estatutaria 1581 por la cual se dictan disposiciones generales para la protección de datos personales y por último la Ley de 1273 de 2009 que penaliza los Delitos Informáticos en Colombia sobre los atentados contra la confidencialidad, la integridad, la disponibilidad de los datos y de los sistemas informáticos. [17]

4.2. MARCO CONCEPTUAL

Seguridad Informática. También conocida como ciberseguridad o seguridad de tecnologías de la información, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes

[16] Kali Linux. . {En línea}. Sistema Operativo. {El 21 de mayo de 2017}. Disponible en: http://www.es.m.wikipedia.org

[17] Sentencia C-831/01. {En línea}. Corte Constitucional República de Colombia. {El 21 de mayo de 2017}. Disponible en: http://www.corteconstitucional.gov.co/relatoria/2001/c-831-01.htm

concebidas para minimizar los posibles riesgos a la infraestructura o a la información. [18]

Sistema de gestión de la seguridad de la información SGSI**.** Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.[19]

Riesgo es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.[20]

Riesgo de seguridad digital es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan. [21]

Gestión de riesgos de seguridad digital**.** Es el conjunto de actividades coordinadas dentro de una organización, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible, los cuales ayudan a

---

[18] WIKIPEDIA. Seguridad de la información (5, noviembre de 2015) [online]; disponible en Internet: https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

[19] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma Técnica Colombiana: NTC-ISO-IEC 27001. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Bogotá: ICONTEC. 2013.

[20] DEPARTAMENTO NACIONAL DE PLANEACIÓN. (2016). *Documento CONPES 3854.* Bogotá, D.C.: Autor.

[21] DEPARTAMENTO NACIONAL DE PLANEACIÓN. (2016). *Documento CONPES 3854.* Bogotá, D.C.: Autor

asegurar que las medidas de gestión de riesgos de seguridad digital sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.[22]

Protocolos de seguridad de la información. Son un conjunto de reglas que gobiernan dentro de la transmisión de datos entre la comunicación de dispositivos para ejercer una confidencialidad, integridad, autenticación y el no repudio de la información. Se componen de:

- Criptografía (Cifrado de datos). Se ocupa de transposicionar u ocultar el mensaje enviado por el emisor hasta que llega a su destino y puede ser descifrado por el receptor.
- Lógica (Estructura y secuencia). Llevar un orden en el cual se agrupan los datos del mensaje el significado del mensaje y saber cuándo se va enviar el mensaje.
- Identificación (*Autentication*). Es una validación de identificación técnica mediante la cual un proceso comprueba que el compañero de comunicación es quien se supone que es y no se trata de un impostor. [23]

Políticas de Seguridad de la Información**.** La falta de coordinación de funciones en las personas encargadas de la protección de los datos es muy común en estas entidades ya que no se cuenta con una dirección o coordinación de un docente que maneje estas políticas fundamentales en las áreas de sistemas o salas de computación, donde se direccionen chequeos a los sistemas de redes y de bases de datos con sismas de backup constantes determinantes evitando perdida de información.[24]

Riesgos Informáticos. El riesgo informático se define como "la probabilidad de que una amenaza en particular expone a una vulnerabilidad que podría afectar a la organización"[25]. Los riesgos informáticos se encuentran presentes cuando confluyen las amenazas y vulnerabilidades, las cuales están íntimamente ligadas y no puede haber ninguna consecuencia sin la presencia conjunta de estas. Las amenazas pueden ser internas o externas, relacionadas con el entorno de las organizaciones; es decir, son los eventos o situaciones que pueden afectar el

[22] Ibíd.
[23] WIKIPEDIA. Seguridad de la información (septiembre de 2016) {En línea}. Disponible en: (https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#Autenticaci.C3.B3n_o_autentific aci.C3.B3n)
[24] Política de seguridad de la información. {05 de octubre de 2017}. Disponible en: (www.datasec.com)
[25] KIM, D., SALOMON, M. G. Fundamentals of Information System Security. Estados Unidos de América: Jones & Bartlett Learning International. 2012. p. 250.

desarrollo de las actividades de las organizaciones, repercutiendo directamente en la información o los sistemas que la procesan. [26]

Las amenazas a la información se pueden agrupar en cuatro categorías a saber, factores humanos (errores, accidentes); fallas en los sistemas de procesamiento de información; desastres naturales y actos maliciosos o malintencionados; algunas de estas pueden ser los virus informáticos, robos de información, fraudes, suplantación de identidad, alteración de la información, espionaje, sabotaje, desastres naturales, entre otros.

Por otra parte, las vulnerabilidades son una debilidad en la tecnología o en los procesos de información; y constituyen el principal elemento de un sistema de información que puede ser aprovechado por un atacante para afectar la integridad, la disponibilidad y la confiabilidad de la información. por lo tanto, las vulnerabilidades son el resultado de errores de programación (bugs), fallos en el diseño del sistema, incluso las limitaciones tecnológicas pueden ser aprovechadas por los atacantes, y se pueden clasificar en físicas, naturales, de hardware, de software, de red y de factor humano.[27]

4.3. ANTECEDENTES

Las Tecnologías de la Información y las Comunicaciones (TIC) actualmente son utilizadas como apoyo y automatización para el desarrollo de las diversas actividades cotidianas; puesto que las empresas han obtenido importantes beneficios en cuanto a la mejora de sus operaciones, optimización de recursos, apertura de nuevos mercados y conocimiento de las necesidades de sus clientes, generando por ello la prestación de servicios de mejor calidad y una comunicación más fluida con todos los participantes de la entidad, permitiendo así aumentar la eficiencia organizacional.

Puesto que con la utilización de las tecnologías de la información y comunicación en las diferentes áreas, se ha propiciado un ahorro de costos y tiempo, y por ende una mejor gestión de los flujos de información; ya que la mayoría de las empresas

[26] TARAZONA, T., César “Amenazas informáticas y seguridad de la información”. {En línea}. {05 de octubre de 2017}. Disponible en: (https:// revistas.uexternado.edu.co/index.php/derpen/article/download/965/915

[27] Madrid Gallego Nicolás. Seguridad y alta disponibilidad. Revisado en: https://nikosad.files.wordpress.com/2011/10/nicolas-madrid-gallego-sad-tema1.pdf

almacenan y documentan sus actividades, procesos, clientes y proveedores en bases de datos, y utilizan internet para comunicarse; por lo que las TIC no soportan solamente las estrategias comerciales existentes en la organización, sino que crea nuevas oportunidades como factor diferencial para obtener ventajas competitivas, a través del valor agregado de los bienes y servicios que la entidad ofrece. [28]

Lo anterior ha conllevado a la dependencia de las organizaciones con las TIC, y más aún en que la mayor parte de la economía se basa en la generación de conocimiento, por lo que depender de la tecnología para el desarrollo de las entidades genera factores y riesgos inherentes al uso de las mismas, como las amenazas tecnológicas (virus informáticos, fallas en el cableado estructurado, etc.), naturales (inundaciones, terremotos, etc.) y humanas (ataque de ingeniería social, malware, etc.); es por esto que las organizaciones han propiciado que sus datos se encuentren seguros en donde los niveles de riesgos informáticos sean aceptables. [29]

Por lo que la utilización de las TIC en las diferentes áreas de las compañías ha propiciado un ahorro de costos y tiempo, ayudándoles a su vez con una mejor gestión de los flujos de información. El Sistema de Gestión de Seguridad de la Información es el concepto principal sobre el cual se centra la norma ISO 27001, la cual consiste en la preservación de la confidencialidad, integridad y disponibilidad de la información dentro de una organización.

Con el propósito de consolidar la seguridad de los datos y sistemas implicados, por lo que es fundamental que todos los integrantes de la entidad participen en la ejecución de este proceso sistemático y documentado, garantizando así que los riesgos de la seguridad de la información sean conocidos, gestionados y minimizados de una forma estructurada, eficiente y adaptada a los cambios que se produzcan en el entorno, las tecnologías y los riesgos empresariales.

---

[28] ICONTEC. {En línea}. Norma Técnica NTC-ISO/IEC Colombiana 27001. {21 de mayo de 2017}. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

29 UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Dirección General de Cómputo y Tecnologías de Información y Comunicación. Revista .Seguridad Cultura de prevención para TI. Número 14. Julio-Agosto 2012. {El línea}. 17 julio 2017. Disponible en: https://revista.seguridad.unam.mx/numero-14/riesgo-tecnol%C3%B3gico-y-su-impacto-para-las-organizaciones-parte-i

La norma ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos; puesto que proporciona la solución de una mejora continua para evaluar los diferentes riesgos y establecer las diferentes estrategias y controles para asegurar la protección y defensa de la información. [30]

Por lo tanto, los Sistemas de Gestión de la Seguridad de la Información (SGSI12) provee un modelo para establecer, implementar, monitorear, revisar, mantener y mejorar la protección de los activos informáticos para lograr los objetivos organizacionales basados en una gestión del riesgo y en los niveles aceptables de riesgos diseñados efectivamente para tratarlos y gestionarlos, analizando los requerimientos para la protección de los activos informáticos y aplicando los controles apropiados para asegurar que la protección de éstos activos contribuyen a la implementación exitosa del mismo.[31]

La norma ISO27001, Sistema de Gestión de Seguridad de la Información, es la solución de mejora continua más apropiada para poder evaluar los diferentes riesgos y establecer una serie de estrategias y controles oportunos para asegurar la protección y defender la información; la cual utiliza el enfoque basado en procesos que usan el ciclo de Deming o el ciclo de mejora continua, consistente en Planificar-Hacer-Verificar-Actuar (PHVA), conocido con las siglas en inglés PDCA. [32] Este modelo consta de las siguientes fases que permiten medir el estado actual del sistema, con el fin de realizar un mejoramiento continuo:

- Planear (Plan): En esta fase se diseña o planea el SGSI, definiendo las políticas de seguridad generales que aplicarán a la organización, los objetivos que se pretenden y cómo ayudarán a lograr los objetivos misionales; de igual manera se realiza el inventario de activos y la selección de la metodología de riesgos a implementar, los cuales deben estar acordes a los objetivos y políticas propuestos.

[30] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma Técnica Colombiana: NTC-ISO-IEC 27001. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Bogotá: ICONTEC. 2013

[31] ISO/IEC. International Standard ISO/IEC 27000: Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary. Geneva: ISO Copyright Office. 2014. p. 13.

[32] GÓMEZ, L., ANDRÉS, A. Guía de Aplicación de la Norma UNE-ISOG/IEC 27001 Sobre Seguridad en Sistemas de Información para PYMES. España: Asociación Española de Normalización y Certificación. 2012.

- Hacer (*Do*): Es la fase donde se implementa el SGSI mediante la aplicación de los controles de seguridad escogidos, asignado los responsables y la ejecución de los procedimientos.
- Verificar (*Check*): Es la fase de monitorización del SGSI donde se verifica y audita que los controles, políticas, procedimientos de seguridad se están aplicando de la manera esperada.
- Actuar (*Act*): Esta fase implementa las acciones correctivas y mejoras del SGSI

De acuerdo con lo anterior, la aplicación de la Norma ISO 27001-2013 propende por la protección de la confidencialidad, integridad y disponibilidad de la información[33] del Colegio Agroindustrial de Puerto Nuevo; a través de la identificación de los diferentes riesgos que pueden afectar la información y el diseño de los mecanismos óptimos para impedir o mitigar sistemáticamente el impacto de los mismos.

4.4. MARCO CONTEXTUAL

4.4.1. Reseña histórica

El Colegio Agroindustrial de Puerto Nuevo fue fundado en el año 2001 para ofrecer la modalidad de básica secundaria y media técnica a los jóvenes del Bajo Simacota, departamento de Santander.

En el año 2012 le fueron asignadas para administrar algunas escuelas del sector entre ellas se encuentran: Escuela rural Sagrado Corazón de Jesús, Escuela rural Marco Fidel Suárez, Escuela rural Puerto Argilio, Escuela rural Maquetalia, Escuela rural Bella Vista y Escuela rural de Zambranito.[34]

Actualmente cuenta con 195 estudiantes en la sede principal de bachiller y aproximadamente con 200 estudiantes en todas las sedes de primaria. La sede principal cuenta con seis aulas de clases, un laboratorio de química y física, un aula múltiple, sala de informática con capacidad para 40 estudiantes, espacio de zonas verdes para proyectos industriales, comedor estudiantil (ofrecen el almuerzo a todos los estudiantes), cancha de microfútbol y baloncesto, y cancha de futbol.[35]

---

[33] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma Técnica Colombiana: NTC-ISO-IEC 27001. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Bogotá: ICONTEC. 2013

[34] Obtenido de la Oficina de Rectoría del Colegio Agroindustrial de Puerto Nuevo Santander

[35] Ibíd.

4.4.2. Misión

El Colegio Agroindustrial de Puerto Nuevo, será una institución Educativa que brindará a la juventud un ciclo tecnológico de carácter agroindustrial, y la orientación de un proceso educativo a los adultos bajo la modalidad de semipresencial en los diferentes programas que ofrece el MEN, dotado de una infraestructura acorde a los avances de la ciencia, con personal docente idóneo, profesional y especializado logrando que entidades privadas y públicas inviertan en los programas académicos, técnicos y científicos, encaminados al desarrollo intelectual, social, empresarial y económico sostenible.[36]

4.4.3. Visión

El Colegio Agroindustrial de Puerto Nuevo es una institución de carácter formal que ofrece educación en los niveles de preescolar, básica primaria, básica secundaria y media técnica con carácter agroindustrial trabajando con el fin de formar lideres competentes en la producción de materias primas, transformación y comercialización de productos terminados a través de la investigación e incorporación de nuevas tecnologías en el desarrollo productivo enmarcados en la organización de su propia empresa.

- Fortalecer el desarrollo de la comunidad apoyando el programa IDEAR dirigido a todos los adultos a toda persona mayor de quince años, que el sistema regular no atiende en nivel de secundaria y en las diversas metodologías para el nivel de primaria.
- Formar personas integras que se destaquen en la práctica del respeto, la responsabilidad, la creatividad, la criticidad y el sentido de pertenencia. [37]

4.4.4. Políticas administrativas

A nivel interno el consejo académico hace uso de los resultados de las pruebas saber o supérate para realizar los planes de área de cada año con el fin de ir anexando los temas más significativos e ir enseñando a los niños el conocimiento al cual tiene derecho. El consejo directivo en cabeza del rector son los encargados de la toma de decisiones del plantel educativo. [38]

---

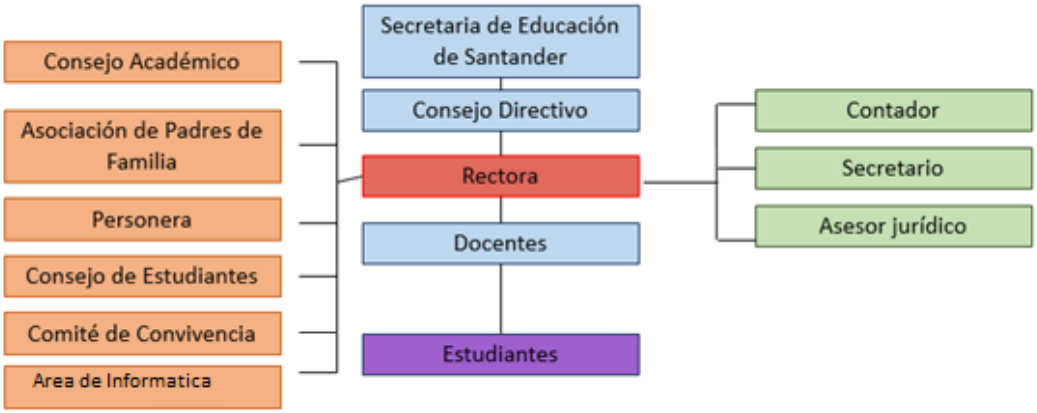
[36] Ibíd.

[37] Obtenido de la Oficina de Rectoría del Colegio Agroindustrial de Puerto Nuevo

[38] Obtenido de la Oficina de Rectoría del Colegio Agroindustrial de Puerto Nuevo

4.4.5. Organigrama Institucional

Fig. 1. Organigrama institucional



Fuente. Obtenido de la Oficina de Rectoría del Colegio Agroindustrial de Puerto Nuevo

4.4.6. Permisos (Ver Anexo A)

Para dar inicio a este estudio y análisis de la problemática presentada y la conclusión de la necesidad de implementación del sistema general de seguridad de la información fue necesario pedir el debido permiso al consejo directivo de la institución educativa, que está encabezado por la rectora.

4.5. MARCO LEGAL

4.5.1. Ley 603 del 2000

Por medio de la cual obliga a las empresas a presentar un detallado informe de gestión, en donde se resalten el tipo de software que usa la compañía, con el fin de proteger la propiedad intelectual y evitar el incremento de la piratería en Colombia. En el artículo segundo de dicha Ley, se faculta a las autoridades tributarias (DIAN) para “verificar el estado de cumplimiento de las normas sobre

derechos de autor, para impedir que a través de su violación, se evadan tributos en cuyo caso iniciara la investigación administrativa correspondiente". [39]

4.5.2. Ley Estatutaria 1266 de 2008

Por la cual se dictan las disposiciones generales del Hábeas Data[40] y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. [41]

Esta Ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personal a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países. [42]

4.5.3. Ley 1273 de 2009

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico utelado - 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. Esta Ley en su capítulo I trata de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos y en su Capítulo II hace referencia de los atentados informáticos y otras infracciones. [43]

4.5.4. Ley 1341 de 2009

Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones. Esta ley tiene como objeto determinar el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la

---

39 Tomado textualmente de la Ley 603 del 27 de julio de 2000 emitida por el Congreso de la República COLOMBIA. CONGRESO DE LA REPÚBLICA

40 Ley de Habes Data. {30 de mayo de 2017}. Revisado en: www.serfinansa.com.co

41 Tomado textualmente de la Ley Estatutaria 1266 del 31 de diciembre de 2008, emitida por el Congreso de la República COLOMBIA. CONGRESO DE LA REPÚBLICA

42 ibíd.

43 Tomado textualmente de la Ley 1273 del 5 de enero de 2009, emitida por el Congreso de la República COLOMBIA. CONGRESO DE LA REPÚBLICA

Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario

También determina lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información. [44]

4.5.5. Ley estatutaria 1581 de 2012

Por la cual se dictan disposiciones generales para la protección de datos personales; dicha Ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. [45]

5. DISEÑO METODOLOGICO

5.1. METODOLOGÍA DE LA INVESTIGACIÓN

El proyecto de aplicación para el diseño del SGSI en el Colegio mencionado, se desarrollara con la total disponibilidad de la docente de informática, utilizando técnicas de investigación del enfoque cuantitativo como: la observación y la hipótesis, también haciendo uso de los instrumentos para recopilar información, como: entrevistas o diálogo con la comunidad educativa y diario de campo. Técnicas que serán abordadas diariamente por la facilidad de acceso que tiene el autor a las instalaciones de la institución, de esta manera se podrá avanzar mayormente y tener a ciencia cierta la solución a la problemática presentada.

5.2. ENFOQUE DE INVESTIGACIÓN

44 Tomado textualmente de la Ley 1341 del 30 de julio de 2009, emitida por el Congreso de la República COLOMBIA. CONGRESO DE LA REPÚBLICA

45 Tomado textualmente de la Ley estatutaria 1581 del 17 de octubre de 2012, emitida por el Congreso de la República COLOMBIA. CONGRESO DE LA REPÚBLICA

Actualmente en el Colegio Agroindustrial de Puerto Nuevo, no existe un sistema que propenda por la seguridad de la información, razón por la cual se hace necesario darle solución a dicha problemática con la implementación del Sistema de Gestión de Seguridad de la Información, por lo que se utilizará el enfoque de investigación cuantitativo, a través de la recolección de datos para probar la hipótesis con base en la medición numérica y el análisis estadístico, y así establecer patrones o relaciones entre las variables.

5.3. TIPO DE INVESTIGACIÓN

Para el desarrollo del presente trabajo se realizara una investigación aplicada de tipo proyecto factible, la cual consiste en la exploración, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas o necesidades de organizaciones o grupos sociales; puede referirse a la formulación de políticas, programas, tecnologías, métodos o procesos. [46] Por lo tanto, se realizará un análisis y desarrollo de la propuesta sobre el diseño de un sistema de gestión de seguridad de la información para el colegio Agroindustrial de Puerto Nuevo Santander, teniendo en cuenta la Norma ISO/IEC 27001:2013.

El Proyecto Factible comprende las siguientes etapas generales: diagnóstico, planteamiento y fundamentación teórica de la propuesta; procedimiento metodológico, actividades y recursos necesarios para su ejecución; análisis y conclusiones sobre la viabilidad y realización del Proyecto; y en caso de su desarrollo, la ejecución de la propuesta y la evaluación tanto del proceso como de sus resultados.[47]

Por lo tanto, en la primera fase se realizará un análisis de la situación actual de la Institución Educativa de Puerto Nuevo, evaluando los riesgos, vulnerabilidades y amenazas encontradas en los activos y recursos del Colegio, con el propósito de evidenciar si existen herramientas para evitar los ataques informáticos.

Seguidamente y teniendo en cuenta los resultados del análisis, se planteará la propuesta de la política de seguridad de la información y por ende el diseño de un sistema de gestión de seguridad de la información a través de la identificación de los procesos y acciones a realizar, las cuales deben estar acorde a las

[46] Manual de Tesis de Grado y Especialización y Maestría y Tesis Doctorales de la Universidad Pedagógica Libertador, Pág.11.
[47] Ibíd.

necesidades de la Institución y del entorno; con el fin de lograr la reducción o eliminación total de los riesgos informáticos en dicho Colegio.

5.4. INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

En el presente trabajo de investigación se utilizarán diversas fuentes bibliográficas, tales como textos, revistas, ebooks, tesis, internet, manuales y demás relacionados, con el propósito de recopilar toda la información necesaria para el desarrollo de este trabajo.

De igual manera, para obtener una información más certera y veraz sobre el manejo de la información en la Institución Educativa, se utilizará la observación directa, encuestas y entrevistas, con el fin de evidenciar y complementar el análisis a realizar en dicha institución.

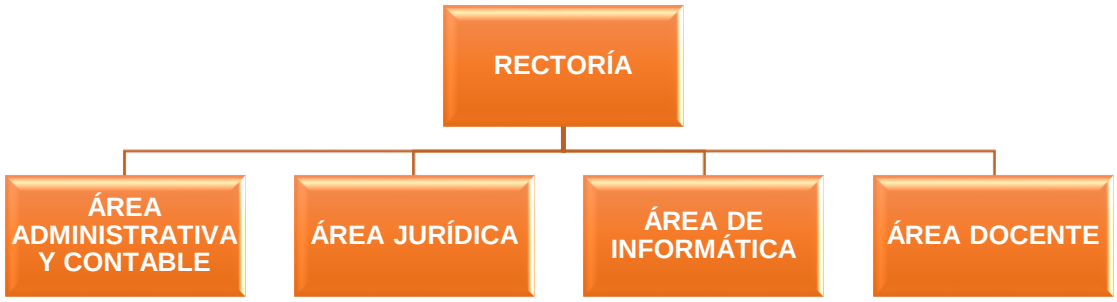
5.5. POBLACIÓN Y MUESTRA

5.5.1. **Población.**

El Colegio Agroindustrial de Puerto Nuevo ubicado en la Vereda La Rochela municipio de Simacota departamento de Santander, ofrece la modalidad de básica secundaria y media técnica a los jóvenes del Bajo Simacota. Tiene asignado a su núcleo seis escuelas de primaria ubicadas en la misma vereda, tales son: Escuela rural Sagrado Corazón de Jesús, Escuela rural Marco Fidel Suárez, Escuela rural Puerto Argilio, Escuela rural Maquetalia, Escuela rural Bella Vista y Escuela rural de Zambranito.

Cuenta actualmente con ciento noventa y cinco (195) estudiantes en la sede principal (bachillerato) y aproximadamente con doscientos (200) estudiantes en todas las sedes de primaria. Este colegio cuenta con las siguientes dependencias:

Fig. 2. Dependencias del Colegio Agroindustrial de Puerto Nuevo Santander



Fuente. Obtenido de la Oficina de Rectoría del Colegio Agroindustrial de Puerto Nuevo

5.5.2. Muestra.

La presente investigación se llevara a cabo en el interior del Colegio Agroindustrial de Puerto Nuevo Simacota, debido a que tanto el personal como activos informáticos son reducidos, lo que hace manejable la aplicación de la metodología a desarrollar para la aplicación del Sistema de Gestión de Seguridad de la Información. Ya que se podrán desarrollar entrevistas y encuestas a la totalidad del personal de la institución, con el fin de revisar los procedimientos implementados, procesos ejecutados, equipos y herramientas involucrados y de esta manera determinar los posibles riesgos y amenazas de la información de la Entidad.

Por lo tanto, la muestra es la siguiente:

Tabla 1. Activos informáticos

Dependencia	Activos Informáticos		Número de personas con acceso a los activos informáticos
	Detalle	Cantidad	
Rectoría	Computador portátil	1	1
Área Administrativa	Computador de escritorio	1	1

Área de Informática	Computadores portátiles	21	45
	Computadores de escritorio	5	

Fuente. El Autor

5.6. METODOLOGÍA DE DESARROLLO

A continuación se presenta cada fase necesaria para el diseño del SGSI según el ciclo de mejora continua PHVA ilustrada en la figura 2. Fases que permite llevar una secuencia de las acciones que se deben realizar como: correctivas, preventivas, evaluación y ejecución.

Fig. 3. Ciclo de mejora continua PHVA

Fuente: http://www.monografias.com/docs112/seguridad-informatica-su-impacto-economico/seguridad-informatica-su-impacto-economico.shtml

5.6.1. Primera fase**.** En esta etapa se realiza el reconocimiento de los sitios y documentos que sean necesarios para diseñar el presente proyecto, estos son:

- Se verifica como se encuentra el área administrativa y académica, encontrando 1 equipo portátil HP y 1 computador de mesa: con sistemas operativo Windows 7, antivirus desactualizado, herramientas informáticas sin licencia y vencidas y además con la infección de virus troyanos.
- Revisión de la contratación del internet de la institución ya que según encuesta realizada están desde el mes de enero sin servicio
- Revisar según los tipos de dispositivos con sus correspondientes manuales

- Manual de funciones de las personas encargadas de administrar los Sistemas de Información.
- Hojas de vida del personal encargado de seguridad de la institución.

5.6.2. Segunda fase. Se procede a analizar la finalidad de la institución educativa, identificando que es de tipo público, enfocada a atender toda clase de población en edad escolar de cero a undécimo grado de forma gratuita, es decir, no tiene fines lucrativos. Luego se analizan los activos, estados del nivel de seguridad de los mismos.

- Visitas a las instalaciones locativas donde se encuentran los activos.
- Revisión e inventario del funcionamiento de los equipos de cómputo que se encuentra en el área administrativa y área académica.[48]

5.6.3. Tercera fase. Verificar los ordenadores con el fin de verificar su operatividad y configuración con el fin de conocer su estado y tipo de sistema. Todo este proceso para implementar la red de datos, escoger el tipo de sistema operativo el cual será una herramienta que se encuentre de manera gratuita en el mercado, como puede ser *Kali Linux* que vienen con aplicaciones completas. Todo esto con el fin de ir avanzando en configuraciones y puesta en marcha de la seguridad de la red, realizando las primeras pruebas de seguridad como pruebas de penetración para reducir los ataques de la información ya que será lo más importante de la institución:

- Se realiza la búsqueda de todas las herramientas de software libre que se podría utilizar *Pentesting y Ethical Hacking*, como por ejemplo de *Kali Linux*.
- Con las herramientas existentes se procede hacer las simulaciones convenientes sobre ataques como: diccionario, acceso no autorizado, vulneración de contraseñas, ping malicioso, revisión de puertas traseras, entre otros.
- Teniendo estos resultados se organiza y se verifican las vulnerabilidades existentes para así definir los controles y salvaguardas.

5.6.4. Cuarta fase. Con las anteriores fases ya trabajadas se procede hacer el diseño del Sistema de Gestión de Seguridad de la Información para el

---

48 BLOGGER de Cyocampo. “El ciclo PHVA Planear – Hacer – Verificar - Actuar”. {En línea}. {21 de Mayo de 2017}. Disponible en: http://lacalidadherramienta.blogspot.com.co/p/el-ciclo-phva-planear-hacer-verificar.html)

Colegio Agroindustrial de Puerto Nuevo, formalizando las responsabilidades de cada sector y los controles a tener en cuenta:

- Implementación de cambios y ejecución de controles
- Formateo de los equipos de cómputo e instalación de nuevo sistema operativo sea *Kali o Windows*
- Instalación de antivirus
- Contratación inmediata del servicio de internet
- Capacitación y divulgación a todo el personal educativo (docente, administrativo), sobre proyecto en marcha, responsabilidades a tener en cuenta y permisos creados.
- Auditorías internas para verificar el buen funcionamiento del SGSI.

6. **DESARROLLO DEL PROYECTO**

Para el desarrollo de este proyecto, fue necesario contar con la aprobación del Consejo Directivo del Colegio Agroindustrial de Puerto Nuevo Santander, el cual dio su aval para realizar el respectivo análisis de la situación actual de la Institución Educativa, así como el establecimiento del Sistema de Seguridad de la Información basados en la Norma ISO 27001:2013; con el fin proteger, detectar y reaccionar ante los diferentes ataques informáticos que se puedan presentar, así

como implementar métodos de detección y procedimientos que permitan salvaguardar la información de dicho plantel educativo.

6.1. PLANIFICACION DEL PROYECTO

La Norma ISO 27001 determina cómo se gestiona la seguridad de la información mediante un sistema de gestión de seguridad de la información – SGSI -. Un sistema de gestión de este tipo se compone de distintas fases que se deben implementar secuencialmente para minimizar los riesgos sobre confidencialidad, integridad y disponibilidad de la información. La primera de las fases es la planificación, ésta sirve para planificar la institución y establecer los objetivos de seguridad de la información y elegir los controles correctos de seguridad. [49]

Se determina el alcance del proyecto que para el caso es Diseñar un Sistema de Gestión de Seguridad de la Información para el Colegio Agroindustrial de Puerto Nuevo del municipio de Simacota (Santander), basado en los requisitos de la norma 27001: 2013.

Inicialmente se realiza un análisis por medio de la observación directa en el cual se recolectan los datos necesarios para reconocer los activos físicos y digitales de la institución; por medio del tipo de investigación Proyecto Factible se desarrollaran las etapas de diagnóstico, planteamiento y fundamentación teórica de la propuesta; procedimiento metodológico, actividades y recursos necesarios para su ejecución; análisis y conclusiones sobre la viabilidad y realización del Proyecto.

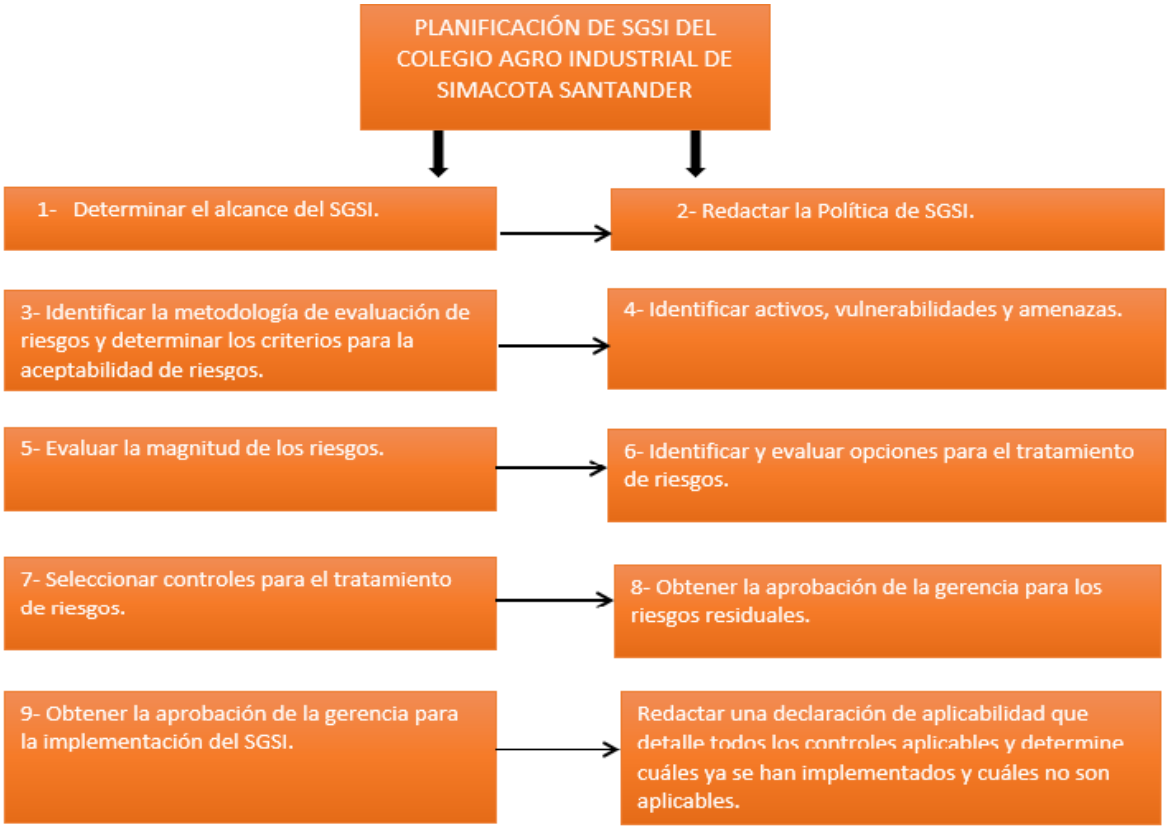
Seguidamente y teniendo en cuenta los resultados del análisis, se identificarán los riesgos a los que están expuestos; sean por disponibilidad al robo de información, daño por causa de desastres naturales (inundación, polvo, terremoto), daño de hardware o dispositivos de almacenamiento, virus o ataques informáticos. El cual permite realizar un análisis y evaluación de los activos de información determinando los activos existentes, las amenazas, las vulnerabilidades y los riesgos a los cuales están expuestos para así determinar las salvaguardas que ayuden a mitigar la probabilidad de impacto que pueden ocasionar.

---

[49] ISOTools Excellence. {En línea}. Implementación de un SGSI etapa 1 Planificación. {El 09 de Mayo de 2017}. Disponible en: http://www.pmg-ssi.com/2014/01/implementacion-de-un-sgsi-etapa-1-planificacion/

Posteriormente se planteará la propuesta de la política de seguridad para asegurar y garantizar la confidencialidad, integridad, y disponibilidad de la información que se utiliza en las dependencias de secretaría, rectoría, sala de profesores y sala de informática, de la información importante del cuerpo administrativo, docentes, estudiantes y comunidad educativa; y por ende el diseño de un sistema de gestión de seguridad de la información a través de la identificación de los procesos y acciones a realizar, las cuales deben estar acorde a las necesidades de la Institución y del entorno; con el fin de lograr la reducción o eliminación total de los riesgos informáticos en dicho Colegio.

Fig. 4. Etapa de planificacion del diseño del SGSI



Fuente. El Autor

6.2. ANÁLISIS DE RESULTADOS

Se procedió a realizar el análisis de los resultados obtenidos en la observación directa, así como en las entrevistas hechas al personal de las diversas áreas del Colegio; con el fin de obtener información del manejo de los datos, activos y recursos con los que cuenta la institución, al igual que el nivel de conocimiento

sobre seguridad y controles para manejar los riesgos por parte de todos los funcionarios del Plantel Educativo.

6.2.1. **Análisis de la observación directa.** La observación directa es un método de recolección de datos que consiste en observar al objeto de estudio dentro de una situación particular. Esto se hace sin intervenir ni alterar el ambiente en el que el objeto se desenvuelve. De lo contrario, los datos obtenidos no serían válidos.[50]

Por tal razón, al observar el funcionamiento del Área de Informática del Colegio Agroindustrial de Puerto Nuevo Santander, se detectaron falencias en el manejo de la información tanto física como digital; así mismo en las dependencias de rectoría, secretaria, sala de profesores y aula de informática se pudo evidenciar que la información se maneja manualmente, sin generar ningún proceso de aseguramiento y control de los datos.

Ante tal situación, se presenta la propuesta de diseñar el SGSI al consejo académico del Colegio, explicando la necesidad de realizar este estudio, ya que permitirá identificar las vulnerabilidades existentes en el manejo y control de la información, así como sugerir el establecimiento de políticas de seguridad que permitan salvaguardar la información de posibles riesgos y ataques informáticos; basados en los requisitos de la norma ISO 27001:2013, para garantizar la confidencialidad, integridad, y disponibilidad del sistema documental de la información de la institución educativa.

De esta manera, se observa en la figura 4, que en la sala de informática del Colegio Agroindustrial de Puerto Nuevo faltan ordenadores y puestos de trabajo para una mejor comodidad de sus alumnos. De igual manera, no se cuenta con acceso a internet, ni aire acondicionado, la sala es muy pequeña y existen grupos de hasta cuarenta (40) estudiantes, por tanto la humedad y la temperatura es inapropiada para el hardware. Así como el grado de hacinamiento existente, lo cual repercute en la incomodidad que tienen los estudiantes al realizar sus labores.

Fig. 5. Sala de informática

[50] LIFEDER. ¿Qué es la observación directa? Características y Tipos. (14 octubre de 2017) [online]; disponible en Internet: https://www.lifeder.com/observacion-directa/

Fuente. El Autor

En la figura 5, se puede observar la puerta de ingreso a secretaria, rectoría y sala de profesores; la cual no cumple con los requisitos exigidos para su seguridad, ya qe no tiene control de acceso, ni cámaras de seguridad; al igual que no cuenta con divisiones entre archivo y sala de profesores.

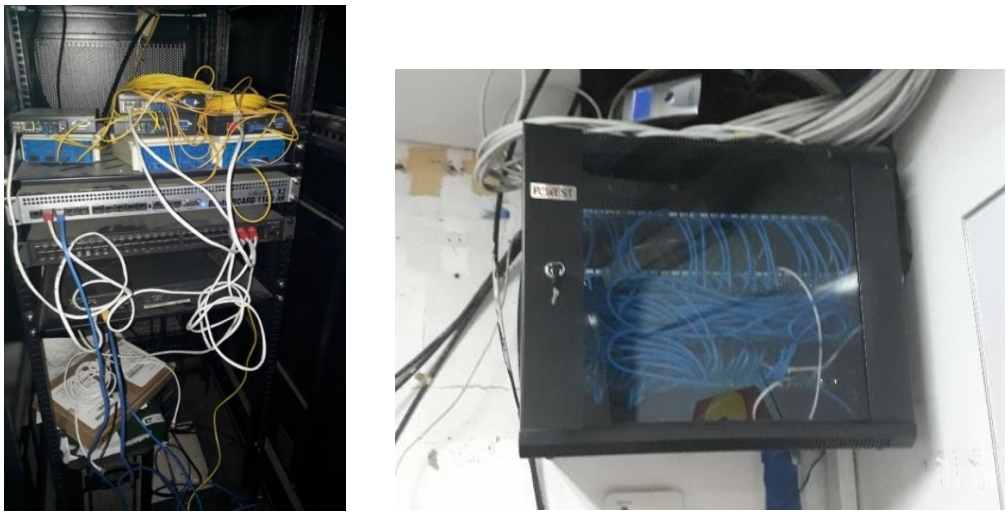
Fig. 6. Puerta de ingreso a las oficinas

Fuente. El Autor

La figura 6 muestra el Rack de la sala de informatica del Colegio Agroindustrial de Puerto Nuevo, la cual no tiene la organización requerida por las políticas de seguridad en el sistema de cableado estructurado y en las redes eléctricas, por

tanto presenta una gran amenaza contra el área de talento humano y la integridad de la información.

Fig. 7. Rack sala de informática (sin servicio de internet)



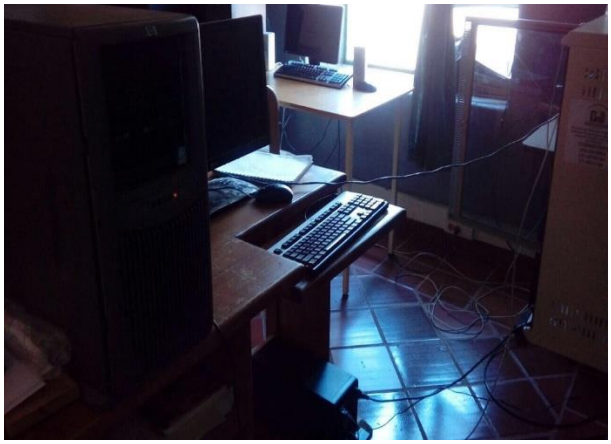
Fuente. El Autor

Fig.8. Oficina de Rectoría

Fuente. El Autor

En la Figura 8 se puede observar la vulnerabilidad existente en la rectoría del Colegio, ante la posible presencia de un incendio, puesto que el equipo informático se encuentra ubicado sobre una mesa de madera, lo cual puede facilitar la propagación del fuego.

Fig. 9. Sala de Profesores



Fuente. El autor

En la figura 9, se puede evidenciar varias vulnerabilidades, como por ejemplo propagación de llamas, en el momento de presentarse un incendio, ya que todos los equipos informáticos se encuentran ubicados en mesas de madera. De igual manera, se puede observar gran desorden, tanto en la ubicación de los computadores como en el cableado; ya que el sitio está rodeado de cables para hacer la conexión al rack, además del peligro de enredarse y caer al entrar o salir del sitio

Fig. 10. Control de incendios

Fuente. El autor

En la figura 10, se puede observar que el Colegio Agroindustrial de Puerto Nuevo Santander, posee extintor manual para control y manejo de fuegos básicos, el cual no

cuenta con gabinete para soportarlo, situación que puede incurrir en algún tipo de accidente.

Fig. 11. Caja de instalaciones eléctrica del Colegio

Fuente. El autor

En la figura 11, se puede evidenciar que el sistema de fluido eléctrico no cuenta con los elementos requeridos, para un mejor manejo de la seguridad de los activos comprometidos en la sala de informática, puesto que al momento de presentarse una amenaza de corto circuito, la Institución no posee el plan de contingencia para superar y evitar este tipo de emergencia.

Fig. 12. Antena de comunicación

Fuente: El Autor

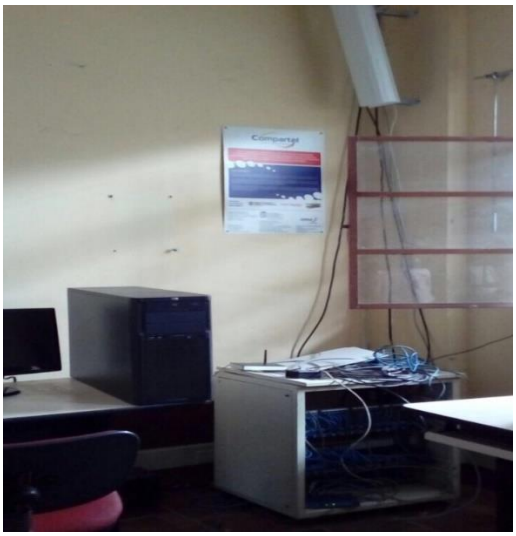
Como se puede observar en la figura 12, el sistema de comunicación no cuenta con una organización estructurada de la conectividad que amerita, para que no se presenten caídas en el sistema, ya que de este depende la estabilidad y el traslado de la información por la red interna de la institución.

Fig. 13. Estabilizador de la sala de informática

Fuente. El autor

En la figura 13 se muestra que la Institución Educativa no tiene un buen manejo en los procesos de interrupción del servicio eléctrico, pues se puede evidenciar que el elemento utilizado no cuenta con un sistema que proporcione un fluido eléctrico de emergencia por determinado tiempo, mientras se realizan los backups de la información.

Fig. 14. Servidor de la Institución



Fuente. El autor

En la figura 14, se muestra el servidor del colegio, el cual se encuentra sobre el suelo, representando una vulnerabilidad en el evento de presentarse una inundación por un desastre natural o por algún daño en el sistema de acueducto de la Institución Educativa. De igual manera, se encuentra ubicado al lado de una ventana, generando un posible riesgo en temporada de lluvias.

Así mismo, sobre el gabinete del servidor se encuentra el modem y el router; evidenciándose un gran desorden en su organización, al igual que no presenta ningún tipo de seguridad, puesto que permanece abierto, facilitando la manipulación de cualquier persona de estos elementos.

6.3. Análisis y evaluación de riesgos de los activos de información

A través del análisis y evaluación de riesgos se determina el alcance de las amenazas actuales y potenciales de los activos de información de la Institución Educativa, así como el riesgo asociado a la información; ya que a través de los resultados obtenidos se identificará los controles adecuados para reducir o eliminar los riesgos durante los procesos de mitigación de los mismos.

Por tal razón y teniendo en cuenta la norma ISO/IEC 27001:2013, se aplicará la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT –versión 3.0[51], como método de análisis y evaluación de los riesgos, vulnerabilidades y amenazas encontradas en los activos y recursos de la Institución, los cuales fueron identificados tanto en la observación directa como en las encuestas realizadas al personal del Colegio Agroindustrial de Puerto Nuevo Santander.

Dicha metodología se desarrolló teniendo en cuenta las siguientes fases:

- Determinar los activos, y sus respectivas amenazas, vulnerabilidades y riesgos.
- Determinar las salvaguardas (o Controles de seguridad) Implantados.
- Estimar el impacto.
- Estimar el riesgo

[51] PAE. Portal administración electrónica. [16 de 09 de 2017]. MAGERIT V.3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II Catálogo de elementos. Recuperado el 16 de 09 de 2017 en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Wb6W9MZrzIV

6.3.1. **Tipos de Activos** (Ver Anexo B)

Tabla 2. Inventario de Activos

Grupo de activo según metodología MAGERTI	Activos Informáticos	Vulnerabilidad	Amenaza	Riesgo
[essential] Activos esenciales	Documentos Boletines			
[D] Datos / Información	Datos internos y externos			
[SW] Software – Aplicaciones Informáticas	Sistema Operativo			
[HW] Equipamiento informático (Hardware)	Computadores Impresoras Cámaras web			
[COM] Red de comunicaciones	Red local			
[Media] Soportes de información	Memorias USB, DVD, Discos duros, material impreso			
[AUX] Equipamiento auxiliar	Aires acondicionado Cableado eléctrico Equipos de oficina			
[P] Personal	Docentes, secretario, estudiantes, rector			
[L] Instalaciones	Infraestructura			

6.3.2. **Vulnerabilidades, amenazas y riesgos de seguridad del área de informática** (Ver Anexo C)

Tabla 3. Vulnerabilidades, amenazas y riesgos de seguridad

Tipo de Amenaza [**N.1**] Fuego	
Tipos de activos **[HW]** Equipamiento informático (Hardware) [**Media**] Soportes de información [**AUX**] Equipamiento auxiliar [**L**] Instalaciones	***Dimensiones*** [**D**] Disponibilidad
Descripción: Amenazas naturales como posibilidad de incendio, terremoto u otros.	

6.4. **Evaluación del nivel de impacto**

De acuerdo con las amenazas identificadas a través de la Metodología MAGERIT, se establece para cada activo su probabilidad o frecuencia de ocurrencia y el impacto que tiene en cada una de las dimensiones de seguridad. En la siguiente tabla se puede observar los factores de amenaza según la clasificación de la metodología MAGERIT, tanto para factores naturales como no naturales. De igual manera, se muestra cuáles son los activos que se ven afectados por cada uno de los factores de amenaza, así como la medición de la frecuencia o probabilidad de ocurrencia y el impacto que causaría de llegar a concretarse.

En cada uno de los activos informáticos que han sido identificados, se debe aplicar la tabla de amenazas y su valoración correspondiente en probabilidad e impacto. Así mismo, se realiza una verificación y Valoración cualitativa de los activos informáticos MAGERIT y la escala de rango porcentual de impactos en los activos.

Tabla 4. Escala de Rango de frecuencia de amenazas.

Vulnerabilidad	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada semana	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Fuente: Metodología Magerit Versión 3.

Tabla 5. Dimensiones de seguridad.

Dimensiones de Seguridad	Identificación
Autenticidad	A
Confidencialidad	C
Integridad	I
Disponibilidad	D
Trazabilidad	T

Fuente: Metodología Magerit Versión 3.

Tabla 6. Escala de Rango porcentual de impactos en los activos para cada dimensión de seguridad.

Impacto	Valor cuantitativo
Muy alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy bajo	5%

Fuente: Metodología Magerit Versión 3.

6.4.1. Resultado Evaluación del nivel de impacto (Ver Anexo D)

Relación de amenazas por activo identificando su frecuencia e impacto							
			Impacto para cada dimensión %				
Amenaza	**Activo**	**Frecuencia**	[A]	[C]	[I]	[D]	[T]
[N.1] Fuego	[host] servidores	**5**				**100%**	
	[otros] dispositivos	**5**				**100%**	
	[pc] Equipo de cómputo de mesa	**5**			**75%**	5%	
	[scan] Equipos de plotter y escanners	**5**			**75%**		
	[HW] EquiposPortatiles	**5**			**75%**		
	[print] Impresoras Lasser	**5**			**20%**		
	[print] Impresoras de inyección de tinta	**5**	5%		**20%**		
	[router] Enrutadores	**5**				**100%**	

6.5. Implementación de salvaguardas

Las ‘SALVAGUARDAS’ se relacionan como aquellas “medidas para anticipar, minimizar, mitigar o tratar de otro modo los impactos adversos asociados a una actividad dada.”

Tabla 7. Efectos y tipo de salvaguardas

Efecto	Tipo
Preventivas: reducen la probabilidad	[PR] preventivas
	[DR] disuasorias
	[EL] eliminatorias

Acotan la degradación	[IM] minimizadoras
	[CR] correctivas
	[RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización
	[DC] de detección
	[AW] de concienciación
	[AD] administrativas

Fuente. Fuente: Metodología Magerit Versión 3.

6.5.1. Salvaguardas (Ver Anexo E)

Tabla 8. Salvaguardas de Soportes de Información almacenamiento Electrónico

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
[v1]	Ups	[A_auxiliar]	Sistemas de Alimen ación ininterrum pida	Preventivas (PR)	Políticas y Normas de Seguridad
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Administrativa s (AD)	Políticas y Normas de Seguridad Información
				Correctivas (CR)	Gestión de incidentes

6.6. Políticas General de Seguridad y privacidad de la Información

El consejo directivo del Colegio Agroindustrial de Puerto Nuevo, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información

buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y la comunidad educativa, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la institución. [52]

Para el Colegio Agroindustrial de Puerto Nuevo la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados. [53]

De acuerdo con lo anterior, esta política aplica a la Institución según como se defina en el alcance, sus funcionarios administrativos, estudiantes, docentes, la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:[54]

- ✓ Minimizar el riesgo en las funciones más importantes de la institución.
- ✓ Cumplir con los principios de seguridad de la información.
- ✓ Cumplir con los principios de la función administrativa.
- ✓ Proteger los archivos físicos, realizando copias de los mismos de manera digital con el fin de crear copias de seguridad.
- ✓ Mantener la confianza de sus estudiantes, docentes, administrativos y comunidad educativa.
- ✓ Apoyar la innovación tecnológica.
- ✓ Proteger los activos tecnológicos.
- ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios, administrativos, docentes, estudiantes y comunidad educativa del Colegio Agroindustrial de Puerto Nuevo
- ✓ Garantizar la continuidad del servicio frente a incidentes.

---

[52] Guía No. 2. Elaboración de la política general de seguridad y privacidad de la información. MINTIC. Tomado de https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf
[53] Manual Políticas de seguridad de la Información. MINTIC. Revisado en http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/M-TI-01-Manual-Politicas-Seguridad-Informacion.pdf
[54] Guía No. 2. Elaboración de la política general de seguridad y privacidad de la información. MINTIC. Tomado de https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

Alcance/Aplicabilidad

- ✓ Esta política aplica a toda la institución, administrativos, docentes, estudiantes y comunidad educativa del Colegio Agroindustrial de Puerto Nuevo.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

A continuación se establecen las 12 políticas de seguridad que soportan el SGSI del Colegio Agroindustrial de Puerto Nuevo.[55]

- ✓ Colegio Agroindustrial de Puerto Nuevo ha decidido analizar, definir, diseñar, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la institución, y a los requerimientos regulatorios que le aplican a su naturaleza.
- ✓ Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, administrativos, docentes, estudiantes y comunidad educativa.
- ✓ Colegio Agroindustrial de Puerto Nuevo protegerá la información generada, procesada o resguardada por los procesos de matrículas, boletines, planes de aula, PEPS, Proyectos, Evaluaciones, Calificaciones y activos de información que hacen parte de los mismos.
- ✓ Colegio Agroindustrial de Puerto Nuevo protegerá la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- ✓ Colegio Agroindustrial de Puerto Nuevo protegerá su información de las amenazas originadas por parte del personal interno o externo a la institución.
- ✓ Colegio Agroindustrial de Puerto Nuevo protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos.

[55] Guía No. 2. Elaboración de la política general de seguridad y privacidad de la información. MINTIC. Tomado de https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

- ✓ Colegio Agroindustrial de Puerto Nuevo controlará la operación de sus procesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- ✓ Colegio Agroindustrial de Puerto Nuevo implementará control de acceso a la información, sistemas y recursos de red.
- ✓ Colegio Agroindustrial de Puerto Nuevo garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- ✓ Colegio Agroindustrial de Puerto Nuevo garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- ✓ Colegio Agroindustrial de Puerto Nuevo garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- ✓ Colegio Agroindustrial de Puerto Nuevo garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Institución, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

El Colegio Agroindustrial de Puerto Nuevo requiere políticas de seguridad de información como tipo de protección administrativo para prevenir sus activos del tipo de amenaza como: fuego, fallo de servicio de comunicaciones, corte del suministro eléctrico, difusión de software dañino, pérdida de equipos, indisponibilidad del personal, entre otros.

Las políticas de seguridad se requieren también para el tipo de protección correctivos con el fin de corregir las amenazas por suplantación de identidad del usuario, acceso no autorizado, modificación deliberada de la información, divulgación de la información y robo; afectando al hardware, software, la red de comunicaciones, los datos e información, las instalaciones, el personal y los equipos de almacenamiento.

Las políticas de seguridad de información van dirigidas a la secretaría de la institución, rectoría, sala de profesores y sala de informática con el fin de que el área administrativa, docentes, estudiantes y comunidad educativa cumplan con los estándares que allí se presentan, tomando roles de responsabilidad para la implementación, aplicación, seguimiento y autorizaciones de la política, dirigido por el consejo directivo del Colegio y el especialista en Seguridad Informática el cual es el responsable de la revisión, aprobación y evaluación de aplicabilidad y el desarrollo para posterior publicación, socialización y capacitación sobre el manejo de estas.

Este proceso permitirá obtener retroalimentación de la efectividad de las políticas, permitiendo así realizar excepciones, correcciones y ajustes pertinentes. Toda la comunidad educativa debe conocer la existencia de las políticas, la obligatoriedad de su cumplimiento y la ubicación física de tal documento, para que sean consultados en el momento que se requieran.

Se establece un periodo de cada seis meses para el monitoreo y mantenimiento de las políticas de seguridad de la información determinando la efectividad y cumplimiento de las mismas y para asegurar que se encuentran actualizadas, integradas y que contiene los ajustes necesarios y obtenidos de las retroalimentaciones.

Si se determina el cumplimiento de la política de seguridad de la información en cuanto esta ha cumplido su finalidad o la política ya no es necesaria en la Institución porque el personal ya la ejecuta para su propia seguridad, entonces se requiere que este retiro sea documentado con el objetivo de tener referencias y antecedentes sobre el tema.

Inicia la vigencia para el cumplimiento de las políticas de seguridad de la información el 15 de enero de 2018, luego de la aceptación, socialización y capacitación de la comunidad educativa.

7. RECURSOS NECESARIOS PARA EL DESARROLLO DEL PROYECTO

Tabla 9. Presupuesto

RECURSO	DESCRIPCIÓN	PRESUPUESTO
Equipo Humano	Dos ingenieros de sistemas	00
Equipos y Software	Depreciación de equipos portátiles	550.000
Viajes y Salidas de Campo	Ida y regreso (Bucaramanga-Puerto Nuevo), Viáticos	450.000
Materiales y suministros	Resma, Fotocopias, CD-ROM, Argollado, lapiceros	50.000
Bibliografía	Se trabaja con bibliografía de la red (Servicio de banda ancha)	50.000
	TOTAL	**$1.100.000**

Fuente. El Autor

8. CRONOGRAMA DE ACTIVIDADES

Tabla 10. Cronograma de actividades

MESES	MARZO				ABRIL				MAYO				JUNIO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICI	
ACTIVIDADES / SEMANAS	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2
Analizar la problemática presentada en la institución educativa	X	X																												
Estudiar los requerimientos de la norma ISO 27001:2013		X																												
Identificar las vulnerabilidades y amenazas de seguridad de información de los activos existentes en la institución		X	X																											
Analizar los riesgos encontrados en base al SGSI		X	X	X																										
Recopilación de información de la comunidad educativa					X	X	X																							
Crear el plan de tratamiento para mitigar los riesgos existentes							X	X																						
Documentar las políticas, programas y procedimientos que se necesiten para mitigar los riesgos de seguridad de la información de la institución								X	X	X																				
Evaluación de cada uno de los anteriores pasos con el fin de dar solución a las fallas encontradas											X	X	X																	
Entrega de Anteproyecto														X	X															
Atención de solicitudes y correcciones																	X	X	X	X										
Capacitación a personal de la institución educativa																					X	X								
Atención a dudas y fallas que se presenten en el inicio del diseño del SGSI																							X	X						

Fuente. El Autor

9. CONCLUSIONES

Durante el proceso de estudio, análisis, comprensión y evaluación del tema se logra cumplir con el objetivo de este proyecto entregando el Diseño de un Sistema de Gestión de Seguridad de la Información al Colegio Agroindustrial de Puerto Nuevo del municipio de Simacota (Santander), basado en los requisitos de la norma 27001: 2013.

El cual fue pensado en hacerlo por la problemática que se observó en dicha institución, encontrando información en lugares de fácil acceso por el personal interno y externo al establecimiento y que además no se encuentra archivada digitalmente por tanto tampoco tiene sus copias de seguridad.

De manera que se realiza un análisis de la situación actual de la Institución Educativa de Puerto Nuevo, acorde a los requerimientos de la Norma ISO 27001:2013, encontrando muchas falencias en el resguardo de la información responsable por parte de directivos, personal administrativo, docentes, estudiantes y comunidad educativa; como por ejemplo boletines, planes de aula, matrículas, PEPS, proyectos, calificaciones y demás información referente al tema.

Por tanto se evaluaron los riesgos, vulnerabilidades y amenazas encontradas en los activos y recursos de la Institución y el nivel de impacto de cada uno de ellos, implementando las debidas salvaguardas para reducir y eliminar el total de los riesgos informáticos.

En consenso y verificando los alcances económicos de la institución se definen las políticas de seguridad de la información acordes con los lineamientos, procesos y requerimientos institucionales, para cumplimiento de todo el personal administrativo, docente, estudiantes y comunidad educativa en general.

De manera que se hace la presentación física del documento ante el Consejo Directivo del Colegio Agroindustrial de Puerto Nuevo, personal administrativo, docentes, estudiantes y comunidad en general el diseño del Sistema de Gestión de Seguridad de la información con el fin de socializar el tema para la posterior ejecución del proyecto.

Al Colegio Agroindustrial de Puerto Nuevo se le recomienda la importancia de su activo más valioso como lo es la información y todos los dispositivos que tiene que ver con el resguardo de ella. Entregando el diseño del sistema de gestión de seguridad se explica los riesgos, las vulnerabilidades y las amenazas que existen; pero también las salvaguardas que pueden implementar para mitigar el riesgo de pérdida, robo o daño de la información, entre ellos la implementación de las políticas de seguridad de la información las cuales son responsabilidad de su cumplimiento por parte del área administrativa, docentes, estudiantes y padres de familia.

De manera que se deja en alerta al consejo directivo de la Institución para que implementen el diseño desarrollado con el fin prevenir y corregir las vulnerabilidades existentes, y contrarrestar los riesgos que existen dando ejemplos como: ingreso a personal no autorizado al archivo físico, desactualización de software y antivirus, no creación de copias de seguridad, información presta al deterioro por moho, polvo o afectación por desastres naturales, falta de conectividad a internet, no adquisición de planta eléctrica, espacios no aptos para el desarrollo de actividades y manejo inadecuado de claves de acceso; entre otros.

BIBLIOGRAFÍA

AGUIRRE CARDONA, Juan David & ARISTIZABAL BETANCOURT, Catalina. “Diseño del Sistema de Gestión de Seguridad de la Información para el grupo empresarial la Ofrenda”. {En línea}. {09 de mayo de 2017}. Disponible en: (repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf)

BLOGGER de Cyocampo. “El ciclo PHVA Planear – Hacer – Verificar - Actuar”. {En línea}. {21 de Mayo de 2017}. Disponible en: http://lacalidadherramienta.blogspot.com.co/p/el-ciclo-phva-planear-hacer-verificar.html)

HERZOG, Pete. “Manual de la Metodología Abierta de Testeo de Seguridad. OSSTMM 2.1”. {En línea}. {5 de mayo de 2017}. Disponible en: (https://radiosyculturalibre.com.ar/biblioteca/INFOSEC/OSSTMM.es.2.1.pdf)

ISO 27000.ES. “El Portal de ISO 27001 en Español”. {En línea}. {5 de mayo de 2017}. Disponible en: (http://www.iso27000.es/herramientas.html).

ISOTOOLS Excellence. “Implementación de un SGSI etapa 1 Planificación”. {En línea}. {09 de mayo de 2017}. Disponible en: (http://www.pmg-ssi.com/2014/01/implementacion-de-un-sgsi-etapa-1-planificacion/)

JARAMILLO, Juan. “Guía de Implementación ISO 27001”. {En línea}. {10 de mayo de 2017}. Disponible en: (https://es.slideshare.net/JuanJaramillo1/gua-de-implementacin-iso-27001).

KOSUTIC, Dejan. “Lista de apoyo para implementación de ISO 27001”. {En línea}. {10 de mayo de 2017}.Disponible en: (https://advisera.com/27001academy/.../lista-de-apoyo-para-implementacion-de-iso-27).

PAE. Portal administración electrónica. [16 de 09 de 2017]. MAGERIT V.3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II Catálogo de elementos. Recuperado el 16 de 09 de 2017 en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Wb6W9MZrzIV

SUING, Abel. “Definición de las Líneas de Investigación”. {En línea}. {25 de abril de 2017}. Disponible en: (https://es.slideshare.net/abelsuing/definicin-de-las-lneas-de-investigacion)

PAE. Portal administración electrónica. [16 de 09 de 2017]. MAGERIT V.3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II Catálogo de elementos. Recuperado el 16 de 09 de 2017 en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Wb6W9MZrzIV

Política de seguridad de la información. {En línea}. {05 de octubre de 2017}. Revisado en: www.datasec.com

MAGERIT 3.0. Metodología de Análisis y Gestión de Riesgos de los sistemas de Información. Libro 1. Madrid. Octubre de 2012.

Portafolio educativo. Información suministrada por secretaría.
DEPARTAMENTO NACIONAL DE PLANEACIÓN. (2016). Documento CONPES 3854. Bogotá, D.C.: Autor

Para el país, la seguridad digital es una política nacional. Revisado en: http://www.portafolio.co

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma Técnica Colombiana: NTC-ISO-IEC 27001. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Bogotá: ICONTEC. 2013.
Información recolectada en la visita que se hace al colegio

PACHECO, Federico, La importancia de un SGSI {En línea}. 03 octubre de 2017. Disponible en: (http://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/)

Sistema de Gestión de la Seguridad de la Información. Procedimientos de Seguridad de la información. MINTIC. Revisado en: http://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

Información recolectada en la visita que se hace al colegio.

ISO/IEC. International Standard ISO/IEC 27000: Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary. Geneva: ISO Copyright Office. 2014. p. 13.

GÓMEZ, L., ANDRÉS, A. Guía de Aplicación de la Norma UNE-ISOG/IEC 27001 Sobre Seguridad en Sistemas de Información para PYMES. España: Asociación Española de Normalización y Certificación. 2012.

Kali Linux. . {En línea}. Sistema Operativo. {El 21 de mayo de 2017}. Disponible en: http://www.es.m.wikipedia.org

Sentencia C-831/01. {En línea}. Corte Constitucional República de Colombia. {El 21 de mayo de 2017}. Disponible en: http://www.corteconstitucional.gov.co/relatoria/2001/c-831-01.htm

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma Técnica Colombiana: NTC-ISO-IEC 27001. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Bogotá: ICONTEC. 2013.

DEPARTAMENTO NACIONAL DE PLANEACIÓN. (2016). *Documento CONPES 3854.* Bogotá, D.C.: Autor.

Política de seguridad de la información. {05 de octubre de 2017}. Disponible en: (www.datasec.com)

KIM, D., SALOMON, M. G. Fundamentals of Information System Security. Estados Unidos de América: Jones & Bartlett Learning International. 2012. p. 250.

TARAZONA, T., César “Amenazas informáticas y seguridad de la información”. {En línea}. {05 de octubre de 2017}. Disponible en: (https:// revistas.uexternado.edu.co/index.php/derpen/article/download/965/915

Madrid Gallego Nicolás. Seguridad y alta disponibilidad. Revisado en: https://nikosad.files.wordpress.com/2011/10/nicolas-madrid-gallego-sad-tema1.pdf

ICONTEC. {En línea}. Norma Técnica NTC-ISO/IEC Colombiana 27001. {21 de mayo de 2017}. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma Técnica Colombiana: NTC-ISO-IEC 27001. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Bogotá: ICONTEC. 2013

ISO/IEC. International Standard ISO/IEC 27000: Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary. Geneva: ISO Copyright Office. 2014. p. 13.

GÓMEZ, L., ANDRÉS, A. Guía de Aplicación de la Norma UNE-ISOG/IEC 27001 Sobre Seguridad en Sistemas de Información para PYMES. España: Asociación Española de Normalización y Certificación. 2012.

Ley de Habes Data. {30 de mayo de 2017}. Revisado en: www.serfinansa.com.co

Manual de Tesis de Grado y Especialización y Maestría y Tesis Doctorales de la Universidad Pedagógica Libertador, Pág.11.

LIFEDER. ¿Qué es la observación directa? Características y Tipos. (14 octubre de 2017) [online]; disponible en Internet: https://www.lifeder.com/observacion-directa/

PAE. Portal administración electrónica. [16 de 09 de 2017]. MAGERIT V.3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II Catálogo de elementos. Recuperado el 16 de 09 de 2017 en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Wb6W9MZrzIV

Guía No. 2. Elaboración de la política general de seguridad y privacidad de la información. MINTIC. Tomado de https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

Manual Políticas de seguridad de la Información. MINTIC. Revisado en http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/M-TI-01-Manual-Politicas-Seguridad-Informacion.pdf

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Dirección General de Cómputo y Tecnologías de Información y Comunicación. Revista .Seguridad Cultura de prevención para TI. Número 14. Julio-Agosto 2012. {El línea}. 17 julio 2017. Disponible en: https://revista.seguridad.unam.mx/numero-14/riesgo-tecnol%C3%B3gico-y-su-impacto-para-las-organizaciones-parte-i

ISO/IEC. International Standard ISO/IEC 27000: Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary. Geneva: ISO Copyright Office. 2014. p. 13.

KIM, D., SALOMON, M. G. Fundamentals of Information System Security. Estados Unidos de América: Jones & Bartlett Learning International. 2012. p. 250

ANEXOS

ANEXO A

CARTA DE ACEPTACION

COLEGIO AGROINDUSTRIAL PUERTO NUEVO
SIMACOTA
RESOLUCIÓN 0015283 de Nov 23 de 2005
TEL: 3112564364
NIT 804016885-8
DANE 268745000781

Puerto Nuevo, bajo Simacota, julio 28 de 2017

Ingenieros
ALIX RUEDA LEON
JOSE DARLING CASTILLO SARMIENTO
L. C.

Respetados ingenieros:

Atendiendo a su oficio con fecha julio 13 de 2017 donde manifiestan el deseo de trabajar en nuestra institución educativa con el proyecto de grado denominado: Diseñar un sistema de gestión de seguridad de la información para el Colegio Agroindustrial de Puerto Nuevo del municipio de Simacota (Santander) basado en los requisitos de la norma 27001:2013, proyecto del cual la institución saldrá beneficiada, me permito responder que acepto la propuesta del desarrollo de su proyecto en este colegio con el compromiso de que dicho sistema sea instalado en el colegio, allegando copia del proyecto.

Deseo éxitos en sus labores personales y profesionales.

Cordialmente,

Luz Amparo Ardila Meneses
Esp.G.I.E.LUZ AMPARO ARDILA MENESES
Rectora
c.c. 43033980 Medellín

ANEXO B

TIPOS DE ACTIVOS

Grupo de activo según metodología MAGERTI	Activos Informáticos	Vulnerabilidad	Amenaza	Riesgo
[essential] Activos esenciales				
[info] Información [per] datos de carácter personal [A] nivel alto [classified] datos clasificados [C] nivel confidencial [pub] de carácter público	Documentos del colegio, datos personales de padres-estudiantes-docentes y grupo administrativo. Calificaciones. Planes de área	NO existe copia sistemática de toda esta información, todo se guarda en físico y en carpetas folder.	El archivo que tiene toda esta información no está en un lugar seguro ya que se encuentra en sala de profesores por lo tanto se permite el ingreso de todo personal.	Robo o pérdida de información. Fallos de confidencialidad. Inseguridad de la información Acceso de personal no autorizado a la información.
[D] Datos / Información				
[int] Datos de gestión interna	Información personal de la comunidad educativa (estudiantes, padres, docentes y personal administrativo)	Información no sistematizada	Riesgo de pérdida de información por inexistencia de dispositivos de almacenamiento de información.	Perdida de información.
		Malas prácticas para registro y almacenamiento de respaldos.	Extravío de la información.	Fallos de confidencialidad y pérdida de la información.
[backup] Copias de respaldo		Back up no existe para restauración de datos.	Imposibilidad de restaurar información comprometida.	Perdida de la información.
[SW] Software – Aplicaciones Informáticas				
[os] Sistema operativo	Sistemas operativos de las estaciones de trabajo y equipos administrativos	Falta de licenciamiento	Revocación o bloqueos por fallos de licencia	Bloqueo operacional o de productividad.
		Actualizaciones del Sistema operativo deshabilitadas.	Posibles backdoor para software malicioso.	Daño del sistema operativo e información del equipo.
[www] servidor de presentación [app] servidor de aplicaciones [ts] servidor de	Servidor	Configuración por defecto para credenciales de administrados y usuarios	Aprovechamiento de credenciales para el acceso a servidor local o remotamente.	Ataque directo o a través de redes.
		Actualización y gestión de aplicaciones	Debug propio de sistemas operativos que pueden ser aprovechados por los atacantes.	Aprovechamiento de fallos propios de sistema operativo

Grupo de activo según metodología MAGERTI	Activos Informáticos	Vulnerabilidad	Amenaza	Riesgo
terminales		Temperatura adecuada de hardware.	Daño en hardware. Ausencia de conectividad a internet.	Fallos en disponibilidad de datos e incluso pérdida.
		Falta de control de licenciamiento	Bloqueos en proceso y fallos de actualización	Bloqueo de procesos.
[HW] Equipamiento informático (Hardware)				
[pc] informática personal [peripheral] periféricos [print] medios de impresión [modem] módems [switch] conmutadores	Computadores portátiles de la sala informática y administrativos. cámaras web, parlantes Impresoras Equipamiento para trasmitir los datos	Dispositivos de almacenamiento defectuoso y desactualizados	Daño de hardware que contiene la información.	Perdida de la información.
[COM] Red de comunicaciones				
[LAN] red local [Internet] Internet	Red local – WLAN	Administración de dominio para compartir recursos. No existe conexión activa a internet.	Desprotección de información en carpetas públicas.	Pérdida de la confidencialidad. Robo de información.
[Media] Soportes de información				
[disk] discos [usb] memorias USB [dvd] DVD	Dispositivos físicos que permiten almacenar información	Dispositivos de almacenamiento defectuoso	Daño de los soportes que tienen la información	Perdida de la información.

Grupo de activo según metodología MAGERTI	Activos Informáticos	Vulnerabilidad	Amenaza	Riesgo
[printed] material impreso				
[AUX] Equipamiento auxiliar				
[ac] equipos de climatización [cabling] cableado [furniture] mobiliario: armarios	Aire acondicionado Cableado eléctrico y de datos Equipos de oficina (escritorios, sillas, etc)	Equipos que se encuentran en mal estado por el transcurrir del tiempo.	Conexión fallida por daño de los equipos	Perdida de la información. Bloqueo de procesos. Retraso en las entregas de los trabajos.
[P] Personal				
[ue] usuarios externos [ui] usuarios internos [op] operadores [adm] administradores de sistemas	Integrantes de grupo de trabajo: docente de informática, estudiantes, rector y secretario.	Ingeniería Social	Develación de información reservada.	Pérdida de la confidencialidad.
[L] Instalaciones				
[site] recinto [building] edificio	Instalaciones	Las instalaciones del área administrativa son cerradas con puertas metálicas, con cielorraso y el área informática tiene una reja de hierro sobre el cielorraso pero en cuando está abierto hay mucho transcurrir de	Acceso de personal no autorizado al archivo físico.	Obtención y publicación de información privilegiada o confidencial.

Grupo de activo según metodología MAGERTI	Activos Informáticos	Vulnerabilidad	Amenaza	Riesgo
		personal.		
[local] cuarto		Las instalaciones y puestos de la sala de docentes están dentro del mismo archivo del colegio por tal motivo se halla expuesto a incendio y robo de información.	Manipulación indebida de los componentes de red. Difusión de software malicioso.	Riesgo de incendio descontrolado.

ANEXO C

VULNERABILIDADES, AMENAZAS Y RIESGOS DE SEGURIDAD DEL ÁREA INFORMÁTICA

Tipo de Amenaza

[**N.1**] Fuego	
Tipos de activos **[HW]** Equipamiento informático (Hardware) [**Media**] Soportes de información [**AUX**] Equipamiento auxiliar [**L**] Instalaciones	***Dimensiones*** [**D**] Disponibilidad
Descripción: Amenazas naturales como posibilidad de incendio, terremoto u otros.	

Tipo de Amenaza **[I.8]** Fallo de servicio de telecomunicaciones	
Tipos de activos [**COM**] Red de comunicaciones	***Dimensiones*** [**D**] Disponibilidad
Descripción: Sea del origen entorno o humano cesa la capacidad de transmitir datos cuando son requeridos por la secretaria de educación.	

Tipo de Amenaza **[I.6]** Corte del suministro eléctrico	
Tipos de activos **[HW]** Equipamiento informático (Hardware) [**Media**] Soportes de información [**AUX**] Equipamiento auxiliar	***Dimensiones*** [**D**] Disponibilidad
Descripción: Interrupción de los procesos, producto de no tener una fuente de energía autónoma y propia como respaldo, cuando el suministro de energía es suspendido por parte del operador.	

Tipo de Amenaza **[E.**8**]** Difusión de software dañino	
Tipos de activos [**SW**] Software – Aplicaciones Informáticas	***Dimensiones*** [**D**] Disponibilidad [I] Integridad [C] Confidencialidad
Descripción: Cuando utilizamos los medios magnéticos en diferentes equipos e inocentemente se propagan virus o Posibles infecciones de virus con origen a la información.	

Tipo de Amenaza	
[E.25] Pérdida de equipos	
Tipos de activos	***Dimensiones***
[HW] Equipamiento informático (Hardware) [**Media**] Soportes de información [**AUX**] Equipamiento auxiliar	[**D**] Disponibilidad [C] Confidencialidad
Descripción: Intrusión de personas con el fin de hurtar, destruir o modificar información o equipos de cómputo.	

Tipo de Amenaza	
[E.28**]** Indisponibilidad del personal	
Tipos de activos	***Dimensiones***
[**P**] Personal	[**D**] Disponibilidad
Descripción: Empleado o docente no asiste a trabajar por enfermedad u otras causas.	

Tipo de Amenaza	
[A.5] Suplantación de identidad del usuario	
Tipos de activos	***Dimensiones***
[**D]** Datos / Información [**SW**] Software – Aplicaciones Informáticas [**COM**] Red de comunicaciones [**Media**] Soportes de información	[**A]** Autenticidad [I] Integridad [C] Confidencialidad
Descripción: Accesos de personal no autorizado a la información o aplicativos.	

Tipo de Amenaza	
[A.11] Acceso no autorizado	
Tipos de activos	***Dimensiones***
[**D]** Datos / Información [**SW**] Software – Aplicaciones Informáticas **[HW]** Equipamiento informático (Hardware) [**COM**] Red de comunicaciones [**Media**] Soportes de información [**AUX**] Equipamiento auxiliar [**L**] Instalaciones	[I] Integridad [C] Confidencialidad
Descripción: Intrusión de personas con el fin de hurtar, destruir o modificar información o equipos de cómputo.	

Tipo de Amenaza	
[A.5] Modificación deliberada de la información	
Tipos de activos [**D]** Datos / Información [**SW**] Software – Aplicaciones Informáticas [**COM**] Red de comunicaciones [**Media**] Soportes de información [**L**] Instalaciones	***Dimensiones*** [I] Integridad
Descripción: Sucede cuando el empleado altera la información por recibir un beneficio.	

Tipo de Amenaza	
[A.19] Divulgación de la información	
Tipos de activos [**D]** Datos / Información [**SW**] Software – Aplicaciones Informáticas [**COM**] Red de comunicaciones [**Media**] Soportes de información [**L**] Instalaciones	***Dimensiones*** [C] Confidencialidad
Descripción: El empleado revela información	

Tipo de Amenaza	
[A.25] Robo	
Tipos de activos **[HW]** Equipamiento informático (Hardware) [**Media**] Soportes de información [**AUX**] Equipamiento auxiliar	***Dimensiones*** [**D]** Disponibilidad [C] Confidencialidad
Descripción: Sucede cuando hay robo de documentos o hardware por personal interno o externo.	

ANEXO D

RESULTADO EVALUACIÓN DEL NIVEL DE IMPACTO

Relación de amenazas por activo identificando su frecuencia e impacto							
		Frecuencia	Impacto para cada dimensión %				
Amenaza	**Activo**		[A]	[C]	[I]	[D]	[T]

[N.1] Fuego	[host] servidores	**5**				**100%**	
	[otros] dispositivos	**5**				**100%**	
	[pc] Equipo de cómputo de mesa	**5**			**75%**	5%	
	[scan] Equipos de plotter y escanners	**5**			**75%**		
	[HW] EquiposPortatiles	**5**			**75%**		
	[print] Impresoras Lasser	**5**			**20%**		
	[print] Impresoras de inyección de tinta	**5**	5%		**20%**		
	[router] Enrutadores	**5**				**100%**	
[N.2] Daños por agua	[host] servidores	**50**		**50%**			
	[pc] Equipo de cómputo de mesa	**10**		**50%**		**50%**	
	[scan] Equipos de escanners	**5**			**50%**		
	[wifi] Ap para Red Inalámbrica	**5**			**50%**		
	[LAN] Red local Switche de 24 puertos	**5**		**100 %**			
	[printed] Carpetas con la documentación de cada estudiante	**10**		**100 %**			
	[building] Instalacion física del plantel	**5**		**100 %**			
[N.7] Desastres naturales. Fenómeno sísmico.	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	**5**					**100%**
	[usb] Almacenamientos en Disco Duro	**5**			**50%**		**100%**
	[printed] Carpetas con la documentación de cada estudiante.	**50**	5%			**100%**	
	[ui] Personal de soporte TI	**5**			**50%**	**100%**	
	[adm] Administrador de sistemas	**5**			**50%**		
	[host] servidores	**5**			**50%**		
	[otros] dispositivos	**5**		**100 %**			
	[pc] Equipo de cómputo de mesa	**10**		**100 %**			
	[scan] Equipos de escanners	**10**			**20%**		**75%**
[I.5] Avería de origen físico o lógico.	[pc] Equipo de cómputo de mesa	**10**					**75%**
	[print] Impresoras Lasser	**10**				**20%**	
	[router] Enrutadores	**50**			**20%**		
	[backup] sistema de backup	**5**		5%	**75%**		

	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	5				50%	
	[building] Instalacion física de la entidad	10	5%		50%	50%	
[I.6] Corte del suministro eléctrico	[host] servidores	5		50%			
	[pc] Equipo de cómputo de mesa	5	100 %		50%		
	[scan] Equipos escanners	50		50%			
	[HW] EquiposPortatiles	10	100 %				
	[app] Servidor de aplicaciones web	5	5%				
[I.7] Condiciones inadecuadas de temperatura o humedad	[host] servidore	5			100 %		
	[pc] Equipo de cómputo de mesa	50				20%	100%
	[print] Impresoras Lasser y tinta	5	5%			20%	
	[wifi] Ap para Red Inalámbrica	10		100 %			
	[LAN] Red local Switche de 24 puertos	5			20%		
	[app] Servidor de aplicaciones	5			75%		
	[printed] Carpetas con la documentación de cada estudiante del plantel.	10	75%				
	[ui] Personal de soporte TI	5			50%		50%
	[adm] Administrador de sistemas	5	5%	50%			
[I.8] Fallo de servicios de comunicaciones	[wifi] Ap para Red Inalámbrica	5		50%			
	[LAN] Red local Switche de 24 puertos	10		50%		50%	
	[Intranet] intranet	5				50%	
	[www] Servicio de internet al que pueden acceder los funcionarios	50		20%			
	[email] Manejo de correos electrónicos	10				20%	
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	5		20%			5%
[I.10] Degradación de los soportes de almacenamiento de la información	[backup] sistema de backup Base de datos	5			50%		
	[backup] Archivo de Copias de seguridad de la información	10				5%	75%
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	5	50%				

	[usb] Almacenamientos en Disco Duro	5					5%
[E.1] Errores de los usuarios.	[pc] Equipo de cómputo de mesa	10		75%		20%	
	[scan] Equipos escanners	50				20%	
	[HW] EquiposPortatiles	5					
	[print] Impresoras Lasser	5			20%		75%
	[print] Impresoras de inyección de tinta	5				5%	
	[os] sistema operativo	10		5%			
	[linux] open Office	50	75%				
	[email] Manejo de correos electrónicos	5				20%	
	[printed] Carpetas con la documentación del plantel.	5		50%			
[E.2] Errores del administrador	[host] servidores	10	20%				20%
	[router] Enrutadores	5				5%	
	[wifi] Ap para Red Inalámbrica	5			20%		
	[LAN] Red local Switche de 24 puertos	10					
		5		50%			
	[os] sistema operativo	5			75%		
	[app] Servidor de aplicaciones	50		5%			
	[password] Contraseñas de acceso de usuarios del sistema	5			50%		20%
	[encrypt] Claves de cifra de Los bancos	10					75%
[E.8] Difusión de software dañino	[host] servidores	5	20%				
	[pc] Equipo de cómputo de mesa	50			75%		
	[HW] EquiposPortatiles	5		20%			
	[os] sistema operativo	10		20%			50%
		5					
	[www] Servicio de internet al que pueden acceder los funcionarios	5			20%		
	[email] Manejo de correos electrónicos	5	20%				
[E.15] Alteración accidental de la información	[linux] open Office	10					20%
		5		20%			
	[files] Información de profesores	5		20%	50%		
	[backup] Archivo de Copias de seguridad de la información	50		20%			

	[password] Contraseñas de acceso de usuarios del sistema	10		75%			
	[email] Manejo de correos electrónicos	5					5%
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	5		50%			
	[usb] Almacenamientos en Disco Duro	5			50%	20%	
	[printed] Carpetas con la documentación de estudiantes y profesores.	10			20%		
[E.18] Destrucción de información	[linux] open Office	5					5%
		5				50%	
	[files] Información de docentes y alumnos	10				20%	
		50	5%			20%	
	[backup] Archivo de Copias de seguridad de la información	5			50%		
	[password] Contraseñas de acceso de usuarios del sistema	5		75%			
	[email] Manejo de correos electrónicos	5				5%	
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	10		20%	20%		
	[usb] Almacenamientos en Disco Duro	5		20%			
	[printed] Carpetas con la documentación de cada proyecto en ejecución	5		20%			
[E.24] Caída del sistema por agotamiento de recursos	[host] servidores	10				5%	
	[pc] Equipo de computo de mesa	5				50%	
	[HW] EquiposPortatiles	5				20%	
	[os] sistema operativo	10				20%	
	[app] Servidor de aplicaciones	50		50%			5%
		5				75%	
[E.25] Pérdida de equipos-Robo	[HW] EquiposPortatiles	5			20%		
	[usb] Almacenamientos en Disco Duro	10	50%				
	[printed] Carpetas con la documentación de cada estuadiante	5			20%		
	[files] Información deprofesores	10	5%				
	[backup] Archivo de Copias de seguridad de la información	50			20%	50%	

	[password] Contraseñas de acceso de usuarios del sistema	5					
[A.5] Suplantación de la identidad del usuario	[pc] Equipo de computo de mesa	10		20%			
	[HW] EquiposPortatiles	5			5%		
		50			5%		50%
	[password] Contraseñas de acceso de usuarios del sistema	10				75%	
[A.11] Acceso no autorizado	[host] servidores	5			50%		
	[adm] Administrador de sistemas	5		20%			
	[printed] Carpetas con la documentación de cada estudainte por grado	50				20%	
	[backup] Archivo de Copias de seguridad de la información	10	75%				
A.24] Denegación de servicio	[host] servidores	5		20%			
	[app] Servidor de aplicaciones	5				75%	20%
	[www] Servicio de internet al que pueden acceder los estuantes	50		20%			
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	10	75%			50%	
[A.26] Ataque destructivo	[host] servidores	5		20%			
	[wifi] Ap para Red Inalámbrica	50			75%		
	[LAN] Red local Switche de 24 puertos	5			20%		75%
		10			20%		
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	10		20%			

ANEXO E

SALVAGUARDAS

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
[v1]	Ups	[A_auxiliar]	Sistemas de Alimen ación ininterrum pida	Preventivas (PR)	Políticas y Normas de Seguridad
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Administrativa s (AD)	Políticas y Normas de Seguridad Información
				Correctivas (CR)	Gestión de incidentes
[V2]	AV	[A-ANTI VIRUS]	Windows Defender original con actualizaciones automática	Preventivas (PR)	Capacitación al personal, en manejo información.
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Administrativa s (AD)	Políticas y Normas de Seguridad Información
				Correctivas(C R)	Gestión de incidentes
	Memorias	[A_Memorias]	Almacenamient o en Memorias USB	Disuasión (DR)	Guardias de seguridad
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Administrativa s (AD)	Políticas y Normas de Seguridad Información
				Correctivas(C R)	Gestión de incidentes

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
[V3]	Mobiliario	[M-mobiliario]	[building]	Preventivas (PR)	Guardias de seguridad
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Correctivas (CR)	Gestión de incidentes
[V4]	Claves de cifra	C-sifrada	Claves de cifra de acceso a la red	Preventivas (PR)	Clasificación y Encriptación de la información
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Correctivas (CR)	Gestión de incidentes
		C_Documentacion	Carpetas con la documentación de los procesos jurídicos	Disuasión (DR)	Guardias de seguridad
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Correctivas (CR)	Gestión de incidentes

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
[V5]	ADMINISTRADOR	[A_sistemas]	Administrador de sistemas	Administrativas (AD)	Clasificación Información confidencial. Políticas de seguridad.
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
[V6]	Interno (a usuarios de la propia entidad)	[S_U_Interno]	Servicios prestados a empleados y estudiantes al interior como haciendo uso de internet.	Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información