POLITICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA INSTITUCIÓN EDUCATIVA LUIS CARLOS GALÁN SARMIENTO, BASADOS EN LA NORMA ISO/IEC 27001:2013

ANA LUCIA GARRIDO SÁNCHEZ
PASCUAL BRAVO LARA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2018

POLITICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA INSTITUCIÓN EDUCATIVA LUIS CARLOS GALÁN SARMIENTO, BASADOS EN LA NORMA ISO/IEC 27001:2013

ANA LUCIA GARRIDO SÁNCHEZ
PASCUAL BRAVO LARA

Monografía de grado para optar al título de
Especialista en Seguridad Informática

Director de Proyecto
Esp. Ing. Freddy Enrique Acosta

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2018

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá D.C., Junio 15 de 2018

Este trabajo está dedicado a las personas que han llenado la vida de alegría, valor y de enseñanza continua; para seguir en el curso de la vida "Mis Hijos": "Enrique Alberto Bravo Garrido y Zaira Lucia Bravo Garrido".

A nuestras madres como fuente de motivación y orgullo.

Gracias a todos!

Ana y Pascual

AGRADECIMIENTOS

Pascual y Ana Lucia expresan sus agradecimientos a:

Ingeniero Alexander Larrahondo por la orientación que dio comienzo a éste trabajo; donde se destaca su disciplina y dedicación a correcciones presentadas durante el proyecto.

Ingeniero Freddy Enrique Acosta por su dedicación de enriquecer, explicar de manera clara y concisa la estructura del trabajo con su gran capacidad de liderazgo y conocimiento en la estructura de anteproyecto y proyecto.

A todos los amigos que insistieron en seguir adelante con éste proyecto para lograr el título deseado.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

Este trabajo de grado tiene como propósito verificar la situación actual de la institución Educativa Luis Carlos Galán Sarmiento, donde se evidencie los activos de la información mediante la metodología de MAGERIT Libro 2, identificando amenazas y vulnerabilidades a los activos y de allí definir controles acordes a la situación presentada, de acuerdo al anexo A de la norma ISO 27001:2013; dando políticas de seguridad a los controles que se definieron.

En el primer capítulo se realiza un diagnóstico al colegio Luis Carlos Galán Sarmiento con el propósito de identificar los tipos de activos más relevantes, según metodología Magerit Libro 2 y de acuerdo a ello se clasifica según su tipo de Información para valorar las dimensiones de seguridad informática a estos activos.

En el segundo capítulo se identifica las amenazas: internas/externas que pueden tener los activos de la institución y el riesgo que puede ocasionar a éstos.

En el tercer capítulo se define los controles acordes para la institución educativa Luis Carlos Galán Sarmiento, de acuerdo al anexo A de la norma ISO 27001:2013.

Por último se propone políticas de seguridad de la información para la Institución Educativa Luis Carlos Galán Sarmiento teniendo en cuenta los controles aplicados de la norma ISO 27001:2013

Palabras clave: Activos, información, seguridad informática, confidencialidad, integridad, disponibilidad, trazabilidad, salvaguardar, vulnerabilidades, amenazas, riesgo.

ABSTRACT

The aim of this degree project is to verify the current situation of the Luis Carlos Galán Sarmiento Educational Institution, where information assets are evidenced through the MAGERIT Book 2 methodology, identifying threats and vulnerabilities to the assets and from there defining controls according to the situation presented, according to Annex A of ISO 27001: 2013; giving security policies to the controls that were defined.

In the first chapter a diagnosis is made to the Luis Carlos Galán Sarmiento school with the purpose of identifying the most relevant types of assets, according to the Magerit Book 2 methodology and according to this, it is classified according to its type of information to assess the dimensions of computer security to these assets.

The second chapter identifies the threats: internal / external that the assets of the institution may have and the risk it may cause to them.

The third chapter defines the appropriate controls for the Luis Carlos Galán Sarmiento educational institution, in accordance with Annex A of the ISO 27001: 2013 standard.

Finally, information security policies are proposed for the Luis Carlos Galán Sarmiento Educational Institution, taking into account the applied controls of ISO 27001: 2013

Keywords: Assets, information, computer security, confidentiality, integrity, availability, traceability, safeguard, vulnerabilities, threats, risk.

GLOSARIO

ACTIVOS: todo aquello que tiene un valor para la organización y que por lo tanto debe protegerse de robos o modificación de intrusos internos y externos[1].

AMENAZAS: es toda vulnerabilidad que está expuesta los activos de la organización y que debe ser protegido permanentemente[2].

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 (DoS).

ANÁLISIS DE RIESGO: el análisis de riesgo que tiene como propósito determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo[3].

AUTENTICIDAD: la legitimidad y credibilidad de una persona, servicio o elemento debe ser comprobable[4].

CICLO PHVA: la utilización continua del PHVA brinda una solución que realmente permite mantener la competitividad de productos y servicios, mejorar la calidad, reduce los costos, mejora la productividad, reduce los precios, aumenta la participación de mercado, supervivencia de la empresa, provee nuevos puestos de trabajo, aumenta la rentabilidad de la empresa.

CONFIDENCIALIDAD: datos solo pueden ser legibles y modificados por personas autorizados, tanto en el acceso a datos almacenados como también durante la transferencia de ellos[5].

DISPONIBILIDAD: acceso a los datos debe ser garantizado en el momento necesario. Hay que evitar fallas del sistema y proveer el acceso adecuado a los datos[6].

GESTIÒN DE INFORMACIÒN: cuya función decisiva consiste en permitir que los principales encargados de adoptar las decisiones cuenten con información

---

[1] DUTRA, Enrique. Seguridad Informática. [online]. 2017. [citado el 26-11-2017]. Disponible: https://enriquedutra.wordpress.com/

[2] SGSI. Sistema de Gestión de Seguridad de la Información. [online]. 2017. [citado el 26-11-2017]. Disponible: http://www.pmg-ssi.com/2015/06/iso-27001-vulnerabilidades-de-la-organizacion/

[3] ISO 27000.ES. Glosario [en línea]. Madrid: El autor, s.f. [citado el 26-11-2017]. Disponible en: http://www.iso27000.es/glosario.html

[4] ISO 27000.ES. Glosario [en línea]. Madrid: El autor, s.f. [citado el 26-11-2017]. Disponible en: http://www.iso27000.es/glosario.html#section10a

[5] DEFINICIÓNABC. Definición de confidencialidad. . [online] s.l.: El autor, s.f. [citado el 26-11-2017]. Disponible en: http://www.definicionabc.com/comunicacion/confidencialidad.php

[6]ISO 27000.ES. Glosario [en línea]. Madrid: El autor, s.f. [citado el 26-11-2017]. Disponible en: http://www.iso27000.es/glosario.html#section10d

en tiempo real en el momento necesario para formarse un juicio claro y adoptar una decisión[7].

INTEGRIDAD: datos son completos, non-modificados y todos los cambios son reproducibles (se conoce el autor y el momento del cambio)[8].

INFORMACIÒN: la información es un recurso que es preciso gestionar de manera efectiva, al igual que los recursos financieros y humanos. Una gestión eficaz de los recursos de información es una condición básica para la buena gestión de las organizaciones[9].

MAGERIT: metodología para el Análisis y Gestión de Riesgos de los Sistemas de Información), metodología creada por el Ministerio de Administraciones Públicas. MAGERIT ofrece un método estructurado y sistemático para la realización de un análisis de riesgos.

Es un tipo de metodología que es una guía de referencia para realizar procesos de análisis de riesgos al igual que provee lineamientos para la gestión de riesgos en sistemas informáticos y todos los aspectos que giran alrededor de ellos en las organizaciones para lograr muchas de las metas planteadas al interior de las mismas y buscando cumplir las políticas de buen gobierno. El proyecto en mención se basa en esta metodología para poder efectuar el proceso de análisis de riesgos logrando identificar los activos, las amenazas, determinar tanto los riesgos como los impactos potenciales y se recomiendan como proceder a elegir las salvaguardas o contra medidas para minimizar los riesgos[10].

METODOLOGÍA DE MAGERIT: es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas.

NORMA ISO/IEC 27001:2013: es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. a primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2[11].

PEI: proyecto Educativo Distrital, Es la carta de navegación de las escuelas y colegios, en donde se especifican entre otros aspectos los principios y fines del establecimiento, los recursos docentes y didácticos disponibles y necesarios, la

---

[7] ISO 27000.ES. El portal de ISO 27001 en español [online]. Madrid: El autor, s.f. [citado el 26-11-2017]. Disponible en: http://www.iso27000.es/iso27000.html

[8] ISO 27000.ES, Glosario, Op. [online]. [citado el 26-11-2017].Disponible en: http://www.iso27000.es/glosario.html

[9] ISO 27000.ES. El portal de ISO 27001 en español [online]. Madrid: El autor, s.f. [citado el 26-11-2017]. ttp://www.iso27000.es/glosario.html#section10i

[10] DEFINICIÓNABC. Definición de Magerit . [online] s.l.: El autor, s.f. [citado el 26-11-2017]. Disponible en: http://www.definicionabc.com/comunicacion/confidencialidad.php

estrategia pedagógica, el reglamento para docentes y estudiantes y el sistema de gestión.

Según el artículo 14 del decreto 1860 de 1994, toda institución educativa debe elaborar y poner en práctica con la participación de la comunidad educativa, un proyecto educativo institucional que exprese la forma como se ha decidido alcanzar los fines de la educación definidos por la ley, teniendo en cuenta las condiciones sociales, económicas y culturales de su medio.

El proyecto educativo institucional debe responder a situaciones y necesidades de los educandos, de la comunidad local, de la región y del país, ser concreto, factible y evaluable[12].

POLITICAS DE SEGURIDAD: es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene la definición de la seguridad de la información desde el punto de vista de cierta entidad[13].

RECURSOS INFORMÀTICOS: todos aquellos componentes de Hardware y programas (Software) que son necesarios para el buen funcionamiento y la Optimización del trabajo con Ordenadores y Periféricos, tanto a nivel Individual, como Colectivo u Organizativo, sin dejar de lado el buen funcionamiento de los mismos.

RIESGO: 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.

REDP: red Integrada de Participación Educativa-Colombia.

SEGURIDAD INFORMATICA: procesos, actividades, mecanismos que consideran las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.

SGSI: un Sistema de gestión de la seguridad de la información, es como su nombre lo expresa un sistema que se encarga de proveer una cantidad de mecanismos y herramientas basados en la norma ISO 27001 y tiene por objetivo conocer al interior de la institución a los que puede estar expuesta la información, define como se deben gestionar los riesgos y debe ser un marco de referencia para la institución el cual debe ser conocido por todo el personal y debe estar

[12] MINISTERIO DE EDUCACIÒN NACIONAL. [online]. república de Colombia. [citado el 26-11-2017]. Disponible en: http://www.mineducacion.gov.co/1621/article-79361.html

[13] UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Políticas de seguridad informática de la organización [online]. México: UNAM, s.f. [citado el 26-11-2017]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap4.html

sometido a una revisión y a un proceso de mejora constante. Los anteriores aspectos deben ser tenidos en cuenta al momento de elaborar las políticas y procedimientos de una organización para evitar pasar por alto aspectos importantes para que así los usuarios y los sistemas realicen sus procedimientos de la mejor manera posible, de forma concreta y clara además se debe tener presente los derechos y límites de usuarios y administradores. Sin embargo antes de realizar cualquier acción para lograr garantizar estos servicios, es necesario asegurarnos de que los usuarios conozcan las políticas para no generar un ambiente de tensión y/o agresión. La seguridad informática esta creada para velar y proteger los activos informáticos, en aras de garantizar la integridad, disponibilidad y confidencialidad de los datos propios de una organización, independiente de su tamaño, tipo o razón social[14].

VULNERABILIDADES: una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:

- ✓ Permitir que un atacante ejecute comandos como otro usuario
- ✓ Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos
- ✓ Permitir a un atacante hacerse pasar por otra entidad
- ✓ Permitir a un atacante realizar una negación de servicio[15].

[14] SEGUINFO. Mejora continua de un SGSI según ISO 27001 [online]. s.l.: El autor, 2006. [citado el 26-11-2017]. Disponible en: https://seguinfo.wordpress.com/2006/11/19/mejora-continua-de-un-sgsi-segun-iso-27001/

[15] ISO 27000.ES. El portal de ISO 27001 en español [online]. Madrid: El autor, s.f. [citado el 26-11-2017]. http://www.iso27000.es/glosario.html#section10v

INTRODUCCIÒN

La seguridad es un tema importante para cualquier empresa, esté o no conectada a una red pública. No solamente es importante, sino que también puede llegar a ser compleja. Los niveles de seguridad que se pueden implementar son muchos y dependerá del usuario hasta donde quiera llegar[16].

Garantizar que los recursos informáticos de una compañía estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos, es una definición útil para conocer lo que implica el concepto de seguridad informática.

En términos generales, la seguridad puede entenderse como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial. En este sentido, es la información el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales[17].

Garantizar la calidad en la gestión de información donde la institución educativa brinda la oportunidad de nuevos horizontes hacia la seguridad informática de nuevas amenazas para los sistemas de información que se maneja como activo productivo de la institución; estableciendo políticas de seguridad a la plataforma educativa y demás archivos en red que actualmente es utilizada por los directivos y profesores; mostrando los riesgos y vulnerabilidades que se puede presentar si se desconoce del problema y presentando las causas que ocasionaría si no se tiene estas políticas de seguridad.

Hoy día la información es el activo más importante de cualquier organización, en ella se basan la toma de decisiones corporativas que definen el presente y futuro de las mismas, este es el recurso más deseado por intrusos, competencia, empleados descontentos y terceros, del cual desean obtener algún beneficio o intención maliciosa. Por lo anterior es significativo realizar un análisis de riesgos que puedan afectar el buen desarrollo de la misma.

En el presente trabajo se hace un diagnostico a los activos de información con la metodología MAGERIT, identificando cada uno en sus diferentes áreas y clasificándolo como información privada, reservada y confidencial; dándole el nivel de seguridad y de impacto que tiene para la institución.

---

[16] BEEKMAN, George. Seguridad Informática. [online]. 1994. [citado el citado 01-06-2017]. Disponible: ttp://problema.blogcindario.com/2008/10/00014-marco-teorico.html

[17] WHITTEN, Jeffrey. Seguridad Informática. [online]. 1994. [citado el citado 01-06-2017]. Disponible: http://problema.blogcindario.com/2008/10/00014-marco-teorico.html

Es importante que tanto la parte administrativa, docentes y estudiantes se involucren hacia la seguridad informática donde es más que la seguridad de la información, pues interviene el conocer el entorno, definir el alcance, identificar procesos, análisis de riesgos, seleccionar objetivos, seleccionar controles, definir metodologías e identificar necesidades que sirvan para el mantenimiento de los activos y permanencia de su originalidad.

1. DESCRIPICIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

Es importante tener una política de seguridad de red bien concebida y efectiva que pueda proteger la inversión y los recursos de información de la compañía. Vale la pena implementar una política de seguridad si los recursos y la información que la organización tiene en sus redes merecen protegerse. La mayoría de las organizaciones tienen en sus redes información delicada y secretos importantes; esto debe protegerse del acceso indebido del modo que los bienes valiosos como la propiedad corporativa y los edificios de oficinas.[18]

Con la norma ISO 27001:2013, se puede demostrar a clientes existentes y potenciales, proveedores y accionistas la integridad de sus datos y sistemas, así como su compromiso con la seguridad de la información. También puede dar lugar a nuevas oportunidades de negocio con clientes preocupados por la seguridad; puede mejorar la ética de los empleados y fortalecer la noción de confidencialidad en todo el lugar de trabajo. Además, le permite reforzar la seguridad de la información y reducir el posible riesgo de fraude, pérdida de información y divulgación.[19]

La secretaria de Educación hace acompañamiento técnico en mantenimiento a través de La Red Integrada de Participación Educativa (Redp) , que hace parte de un proyecto Transformador Pedagógico de la Escuela y la enseñanza; donde ésta maneja todo el sistema informático.

Debido a los múltiples riesgos y amenazas que está expuesta la institución, es necesario que el colegio cuente con estrategias se seguridad mediante un conjunto coherente de procesos que ayuden a garantizar su Misión y visión, mejorar su imagen, disminuir costos y cumplir las normas establecidas.

Es importante proteger todos los activos que reposan en la parte administrativa de la institución ya que la red de computadores es vulnerable por ser compartida; de ésta manera se presta para alterar o borrar la información por posibles amenazas de agentes internos y externos.

El Colegio Luis Carlos Galán cuenta con unos tipos de activos internos, de aplicaciones, de equipos, de comunicaciones, soporte de información, equipamiento auxiliar, instalaciones y personal que se debe cuidar, proteger y

---

[18] ALVAREZ, Daniel. Seguridad en Informática. [en línea]. En: Maestro en Ingeniería de sistemas empresariales. p.7. [citado el 24-05-17].Disponible en http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

[19] ISO 27001. Sistema de gestión de la seguridad de la información [en línea]. Colombia 1995. [citado el 24-05-17]. Disponible en: http://www.sgs.co/es-ES/Health-Safety/Quality-Health-Safety-and-Environment/Risk-Assessment-and-Management/Security-Management/ISO-27001-2013-Information-Security-Management-Systems.aspx

brindar soporte continuo para detectar vulnerabilidades y crear mantenimiento de soporte.

1.2 FORMULACIÓN DEL PROBLEMA

¿Mediante generación de políticas de seguridad de la información dentro de la institución educativa Luis Carlos Galán Sarmiento, cómo se puede mitigar los riesgos a los que se encuentran expuestos los activos de información y con esto minimizar la fuga de información?

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Proponer políticas de seguridad de la información dentro de la institución educativa Luis Carlos Galán Sarmiento, basadas en la norma ISO/IEC 27001:2013

1.3.2 OBJETIVOS ESPECIFICOS

- ✓ Verificar la situación actual de la Institución Educativa Luis Carlos Galán Sarmiento.
- ✓ Evidenciar los activos de la información de la Institución educativa Luis Carlos Galán Sarmiento mediante la metodología de MAGERIT
- ✓ Identificar amenazas y vulnerabilidades a los activos de la información de la Institución Educativa Luis Carlos Galán Sarmiento mediante la metodología de MAGERIT.
- ✓ Definir cuales controles son acordes para la Institución Educativa Luis Carlos Galán Sarmiento, de acuerdo al anexo A de la norma ISO 27001:2013
- ✓ Proponer políticas de seguridad de la información para la Institución Educativa Luis Carlos Galán Sarmiento teniendo en cuenta los controles aplicados de la norma ISO 27001:2013

1.4 JUSTIFICACIÓN

Las políticas de seguridad de Información basado en el modelo de las buenas prácticas como es la norma ISO 27001:2013 mediante la metodología de MAGERIT, proveerán un análisis y gestión a todo aquello que se trabaje bajo la información digital y sistemas informáticos de gran valor para la institución educativa; el conocer el riesgo de cada activo del Colegio Luis Carlos Galán Sarmiento es ayuda para protegerlos.

La información es el activo más importante en toda organización, y en este mundo digital en el que vivimos y en especial en el ámbito empresarial, esta debe ser protegida ante las crecientes y constantes amenazas a las que está expuesta

por parte de delincuentes informáticos, los cuales tratan de apoderarse de esta ya sea para sacar beneficio económico al venderla o al apoderarse de números de cuentas y claves de usuarios bancarios, sacar provecho de esta información para apropiarse del dinero de los clientes [20].

Pero no solo se debe proteger la información del ataque de delincuentes externos a las organizaciones, también lo directivos de estas empresas deben mirar hacia el interior, en especial hacia sus empleados ya sea que estos manipulen o no información confidencial pues estos son los que tienen disponibles de primera mano este activo tan fundamental denominado información[21].

El control interno informático siendo un conjunto de principios, procesos, procedimientos, políticas, basándose en las políticas preestablecidas, garantiza que se minimice la ocurrencia de riesgos y sus posibles consecuencias, lo que conlleva mediante la presentación de informes que presenten oportunidades de mejora, mejorar la eficiencia y eficacia de los procesos para prevenir la ocurrencia de riesgos, fortaleciendo los procesos al realizar la gestión adecuada de los riesgos identificados[22].

El rápido avance de la tecnología y de las comunicaciones ha permitido a diferentes entidades de sector público y privado, de producción, de servicios y financiero globalizar los procesos, el almacenamiento de información y la ejecución de programas, procesos y procedimientos en tiempo real para prestar más y mejores servicios a sus usuarios y clientes. Considerando que la información es uno de los principales activos de una organización y su importancia en la toma de decisiones, se requiere aplicar herramientas consistentes, reconocidas y aprobadas, para minimizar los riesgos a la integridad, la confidencialidad y a la oportunidad de la información y de todos los elementos utilizados en su almacenamiento, organización, administración y control de esa información.

Es importante minimizar los riesgos, amenazas y vulnerabilidades que se puedan presentar en un sistema de información sobre los datos, medios de almacenamiento, elementos de proceso, comunicación y transmisión, operación y además, como factor importante, sobre todas las personas y sus niveles de acceso a consultar, modificar, adicionar y/o suprimir información.

Con todo este aporte que brinda las políticas de seguridad informática es necesario que la institución Educativa Luis Carlos Galán Sarmiento haga propuestas que garanticen el buen uso de la información para mitigar riesgos a

---

[20] AUDISIS. Sistema de gestión de seguridad de la información - SCSI ISO 27001:2013 - Implantación y auditoría. [en línea]. Bogotá. Disponible en: http://www.audisis.com/BROCHURE_Sem_Implementaci%C3%B3n_SGSI.pdf

[21] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Fortalecimiento de la gestión TI en el estado [en línea]. Bogotá. http://colnodo.apc.org/apropiacionTecnologias.shtml

[22] ISO 27000.ES. Sistema de gestión de la seguridad de la información [en línea]. Madrid.Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

los que se encuentran expuestos los activos de la institución y bajar la fuga de información; por tanto es responsabilidad vital del rector y parte administrativa de ir dialogando de los cambios que se presentará en la institución por motivo de seguridad a la información.

Este proyecto utilizara la metodología de MAGERIT que ofrece un método estructurado y sistemático para la realización de un análisis de riesgos que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones permitiendo así implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados. Esta metodología también cuanta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos.

MAGERIT se basa en analizar el impacto que puede tener la empresa en la violación de la seguridad, buscando identificar las amenazas que pueda llegar afectar la empresa y las vulnerabilidades que pueden ser utilizadas por dichas amenazas, obteniendo un resultado final la identificación clara de las medidas preventivas y correctivas apropiadas que debe contar la entidad.

Los ingenieros encargados de dicha investigación y elaboración de propuesta de políticas de seguridad de la información para la institución educativa Luís Carlos Galán Sarmiento, basados en la norma ISO/IEC 27001:2013 es Ana Lucia Garrido Sánchez y Pascual Bravo Lara.

1.5 ALCANCES Y LIMITACIONES

1.5.1 Alcance

La presente monografía se encuentra entre los proyectos de gestión de la seguridad informática y lo que pretende es generar políticas de seguridad de la información para la institución educativa Luis Carlos Galán Sarmiento, basados en la norma ISO/IEC 27001:2013.

1.5.2 Limitaciones

Es conveniente resaltar que el desarrollo de la presente monografía no abarcara temas como los que se definen a continuación:

- ✓ Por confidencialidad en el proyecto final la razón social de la institución educativa se mantendrá en reserva.
- ✓ No se realizará implementación del sistema gestión en la institución educativa.
- ✓ No se elaboraran check list.
- ✓ No se implementara las políticas de seguridad en la Institución Educativa, pero se entregara el documento para que sea estudiado por las directivas del colegio.
- ✓ No se realizara capacitaciones ni concientizaciones con la comunidad educativa.

1.6 DISEÑO METODOLOGICO

1.6.1 Unidad De Análisis

La unidad de análisis será la Institución Educativa “Colegio Luis Carlos Galán”, Bogotá.

1.6.2 POBLACIÓN Y MUESTRA

1.6.2.1 Población

El presente proyecto tomara como población al Colegio Luis Carlos Galán”, Bogotá; pues es aquí donde está el interés.

1.6.2.2 Muestra

Se estima que para el estudio en referencia, se involucren 3 secretarios 5 coordinadores, 60 docentes y 1 rector; teniendo en cuenta los procesos operativos y administrativos del colegio para entender la problemática de seguridad.

1.6.3 ESTUDIO METODOLÓGICO

Con el fin de desarrollar satisfactoriamente la presente propuesta se ha contemplado Nivel perceptual y el Nivel compresivo para dicha investigación

1.6.3.1 Nivel perceptual

El nivel perceptual hace referencia al tipo de investigación Exploratoria y descriptiva de la situación actual de la Institución Educativa Luis Carlos Galán Sarmiento.

1.6.3.2 Investigación Exploratoria

Es el primer acercamiento científico a un problema. Se utiliza cuando el problema no ha sido abordado o estudiado y las condiciones existentes no ha sido determinadas.[23]

Integra el estadio exploratorio y chequea la presencia de estudios descriptivos, comparativos, analíticos y explicativos Plantea un enunciado predictivo Detecta un evento a predecir[24]

---

[23] HERNANDEZ, Marisol. Metodología de la Investigación. Disponible en: http://metodologiadeinvestigacionmarisol.blogspot.com.co/2012/12/tipos-y-niveles-de-investigacion.html

[24] Córdoba Martha. Tipos de Investigación. Disponible en: http://2633518-0.web-hosting.es/blog/didact_mate/9.Tipos%20de%20Investigaci%C3%B3n.%20Predictiva%2C%20Proyectiva%2C%20Interactiva%2C%20Confirmatoria%20y%20Evaluativa.pdf

1.6.3.3 Investigación descriptiva

Esta investigación se lleva a cabo cuando se describe todos los componentes principales a una realidad.

1.6.3.4 Nivel comprensivo

El nivel hace referencia al tipo de investigación explicativa, predictiva y proyectiva.

1.6.3.5 Investigación proyectiva

Consiste en el diseño predictivo, Operacionaliza eventos, Selecciona las unidades y elabora instrumentos como solución a la necesidad propuesta.[25]

Tiene como objetivo diseñar o crear respuestas dirigidas a resolver determinadas situaciones. Los proyectos de arquitectura e ingeniería, el diseño de maquinarias, la creación de programas de intervención social, el diseño de programas de estudio, los inventos, la elaboración de programas informáticos, etc., son ejemplos de investigación proyectiva, este tipo de investigación potencia el desarrollo tecnológico.[26]

[25] HURTADO DE BARRERA, Jacqueline. Guía para la comprensión holística de la ciencia. 3a ed. Caracas: Fundación Sypal, 2010. p. 132.

[26] Córdoba Martha. Tipos de Investigación. Disponible en: http://2633518-0.web-hosting.es/blog/didact_mate/9.Tipos%20de%20Investigaci%C3%B3n.%20Predictiva%2C%20Proyectiva%2C%20Interactiva%2C%20Confirmatoria%20y%20Evaluativa.pdf

2. MARCO DE REFERENCIA

2.1 MARCO TEORICO

2.1.1 Magerit V3.0, libro 2

Metodología de análisis de riesgos desarrollada por el Ministerio de Administraciones Públicas español, la cual especifica los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación; puntualizando las tareas para realizarlo de forma tal que el proceso esté siempre bajo control contemplando aspectos prácticos para un análisis y una gestión realmente efectivos.[27]

Esta metodología cuenta con catálogos minuciosos de amenazas, vulnerabilidades y salvaguardas. Además, con una herramienta, denominada PILAR para el análisis y la gestión de los riesgos de los sistemas de información con dos versiones, para grandes y pequeñas organizaciones.

2.1.2 Activo de Información

Las organizaciones poseen información importante que se desea proteger frente a cualquier riesgo o amenaza.

Los activos de información son ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo calefacción, iluminación, energía y aire acondicionado y las personas, que son al fin y al cabo las que en última instancia generan, transmiten y destruyen información, es decir dentro de un organización se han de considerar todos los tipos de activos de información[28].

2.1.3 Amenazas

Una amenaza se representa a través de una persona, una circunstancia o evento, un fenómeno o una idea maliciosa, las cuales pueden provocar daño en los sistemas de información, produciendo pérdidas materiales, financieras o de otro tipo. Las amenazas son múltiples desde una inundación, un fallo eléctrico o

---

[27] MARTOS, Fernando. Centros Hospitalarios de Alta Resolución de Andalucía-Auxiliares Administrativos. Primer Edición. España.2006. 195 p. Recuperado de: https://books.google.com.co/books?id=SmwP1cZdI4cC&pg=PA195&dq=LA+METODOLOG%C3%8DA+MAGERIT+3.0&hl=es&sa=X&ved=0ahUKEwiK5d7u_KTJAhUJWCYKHadoB14Q6AEIJTAC#v=onepage&q=LA%20METODOLOG%C3%8DA%20MAGERIT%203.0&f=false

[28] POVEDA, José Manuel. Los activos de seguridad de la información [en línea]. Chile: World Visión, s.f. [citado el 10 de Diciembre de 2017]. Disponible en: http://www.worldvisioncapacitacion.cl/wpcontent/uploads/cursos_adjuntos/f52e0bd4c6c2c203413952826f916237.pdf 27

una organización criminal o terrorista. Así, una amenaza es todo aquello que intenta o pretende destruir[29].

Se considera una amenaza, a cualquier situación que pueda dañar o deteriorar un activo, impactando directamente cualquiera de las cuatro dimensiones de seguridad. La ISO/IEC 13335-1:2004 define que una "amenaza es la causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización".

Las amenazas se clasifican en:

- De origen natural: son eventos naturales que son peligrosos al hombre y que están causados por fuerzas extrañas a el. Como por ejemplo inundaciones, terremotos.

- Origen industrial: son eventos industriales que pueden ocurrir de forma accidental, o por la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

- Errores y fallos no intencionados: son eventos que pueden ocurrir por errores humanos no intencionados. Por ejemplo no saber utilizar una base de datos puede ocasionar la pérdida de algún registro por no saber utilizar el sistema.

- Ataques intencionados: son eventos que pueden ocurrir con el hombre ya que estos pueden provocar intencionalmente que se dañe un sistema.

2.1.4 Seguridad de la Información[30]

La información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades (véase también OECD Guía para la seguridad redes sistemas de información). La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida.

La seguridad de la información se alcanza implementando un conjunto adecuado de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales

[29] UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Fundamentos de seguridad informática: amenazas [en línea]. México: UNAM, s.f. [citado el 10 de Diciembre de 2017]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/Amenazas.php

[30] ESTÁNDAR INTERNACIONAL ISO/IEC 17779. Tecnología de la información - Técnicas de seguridad - Código para la práctica de la gestión de la seguridad de la información [en línea]. s.l.: s.n., 2005. [citado el 10-12-17]. Disponible en: https://mmujica.files.wordpress.com/2007/07/iso17799-2005-castellano.pdf

específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio.

2.1.5 Seguridad Informática

"La seguridad informática es un camino, no un destino". Son las políticas, técnicas y procedimientos para asegurar la confiabilidad, integridad y disponibilidad de los datos que están expuestos a amenazas; de mantener y proteger los sistemas de la empresa (Hardware, software, datos).[31]

La seguridad informática encierra todos esos elementos que involucra en la inseguridad de los sistemas como son: vulnerabilidades, amenazas, riesgos; es importante hacer rastreo y control constante para vigilar el tráfico y evitar sospechas de robo o Delito de confidencialidad e integridad de datos. El estudio de riesgos es importante para saber qué tanto es seguro los sistemas o precauciones debo hacer para que lo sea.[32]

La importancia de los sistemas de información es un papel interesante en las organizaciones, alcanzando a depender de éstas, que ha estimulado la atención a los sistemas TI. Estos sistemas de información se diseñan a partir de necesidades del negocio, empresas/instituciones, Por este motivo los objetivos de la organización es la dependencia de sus sistemas de información.

Hace imprescindible garantizar el funcionamiento de la seguridad de los sistemas de información en las organizaciones. En este informe se pretende dar la importancia de asegurar los sistemas TI y así mismo analizar los riesgos que éstos corren. Para ello se explicara que es un análisis y gestión de riesgos y las múltiples maneras de realizarlo y lo que se pretende con él. Una vez explicadas las distintas formas de hacer un análisis de riesgos se explicara la metodología MAGERIT (Metodología para el Análisis y Gestión de Riesgos de los Sistemas de Información), metodología creada por el Ministerio de Administraciones Públicas. MAGERIT ofrece un método estructurado y sistemático para la realización de un análisis de riesgos.[33]

Las organizaciones forzadas por el aumento de incidentes de seguridad de la información que pueden ocasionar pérdidas ya sea de tipo económico o de información, las cuales a su vez afectan el buen nombre y la permanencia de las mismas en el mercado, por tal motivo éstas se ven obligadas a implementar Sistemas de Gestión de Seguridad de la Información mediante los cuales, se realice la documentación, implementación y monitoreo de controles mediante

---

[31] MEDINA, Johanna. ESTANDARES PARA SEGURIDAD DE INFORMACIÒN CON TECNOLOGIA DE INFORMACIÒN: Información y control de gestión. [en línea]. [citado el 2-06-17]. Disponible en http://www.tesis.uchile.cl/tesis/uchile/2006/medina_j/sources/medina_j.pdf

[32] GONZALEZ, DanielF. EL RIESGO Y LA FALTA DE POLITICAS DE SEGURIDAD INFORMÁTICA UNA AMENAZA EN LAS EMPRESAS CERTIFICADAS BASC. Administración de la seguridad y salud Ocupacional. [en línea]. [citado el 2-06-17]. Disponible en http://repository.unimilitar.edu.co/bitstream/10654/12251/1/ENSAYO%20FINAL.pdf

[33] OLATE, María y PEYRIN, Oscar. SISTEMA DE INFORMACIÒN ESTRATEGICOS Y TECNOLOGIA DE LA INFORMACIÒN. Escuela de Sistemas de Información y autoría. [en línea]. [citado el 2-06-17]. Disponible en http://www.tesis.uchile.cl/tesis/uchile/2004/olate_m/sources/olate_m.pdf

gestión de riesgos encaminados a minimizar tanto el impacto como la probabilidad, buscando mantenerlos en niveles aceptables para la Organización. En tal sentido es pertinente instituir, implementar, conservar y optimar un Sistema de Gestión de Seguridad de Informática (SGSI), el cual considere aspectos tanto físicos como lógicos a fin de efectuar el adecuado tratamiento del riesgo.

En consecuencia el riesgo y control informático en la seguridad de la información involucra no solo recursos económicos como tal sino la inversión de tiempo, esfuerzo y otros recursos que regularmente no están presupuestados en las organizaciones. Sin embargo las Empresas que tienen claridad del valor de sus activos de información, invierten en gestión del riesgo, implementando regularmente normas de la familia ISO 27000, en especial la norma ISO 27005, la cual forma parte de los estándares internacionales que se encarga de la gestión de riesgos de seguridad de información. Referida norma detalla las directrices para llevar a cabo el proceso de gestión del riesgo, misma que es aplicable a todo tipo de Empresa cuyo objetivo sea el de gestionar los riesgos que amenacen la seguridad de la información en su compañía[34].

No obstante las el estándar ISO 27000 no recomienda una metodología concreta. En tal sentido se hace necesario definir y seguir una metodología que se adapte a la Organización en el proceso de gestión del riesgo de una forma mucho más económica en comparación con la inversión que deba hacer para recuperarse de las afectaciones ante la materialización de los riesgos.

De otra parte no se puede hablar de riesgo, si no se conoce qué se quiere proteger, qué valor tiene y contra quien o que se quiere proteger, por tanto debemos iniciar por identificar los activos de información y partiendo de ellos identificar los riesgos que pueden afectar a cada uno de ellos, determinar el grado e impacto. El riesgo es una equivalencia en la cual se relacionan los activos, las amenazas, las vulnerabilidades y el impacto de estas sobre los activos de información. Por consiguiente la evaluación de los riesgos facilita la medición cuantitativa o cualitativa de los mismos. El paso a seguir es la Gestión de los Riegos, donde se determinan las acciones a aplicar, entre otras si se va realiza tratamiento sobre los riesgos, el cual está enfocado a la disminución del nivel del mismo, la transferencia a otra entidad que se encargue de ellos o la aceptación de éste.

La metodología que se ha adoptado para ello es la de MAGERIT, la cual es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como alternativa a la percepción de que las empresas y, en general la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión. Se adopta MAGERIT en razón a la generalización del uso de las tecnologías de la información, que prometen beneficios importantes para todos; sin embargo esta

[34] METODOLOGIA PARA LA GESTIÒN DE LA SEGURIDAD INFORMÀTICA. [en línea]. [citado el 2-06-17]. Disponible en http://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

también trae consigo riesgos, los cuales necesitan ser minimizados aplicando medidas de seguridad encaminadas a generar confianza en la organización.

El objetivo de la referida metodología está orientado a determinar los riesgos a fin de proceder a minimizarlos o de ser posible eliminarlos, por medio de la implementación de controles de seguridad. Es pertinente recalcar que en la Gestión de Riegos se enfatiza en el estudio de "costo – beneficio", por cuanto el valor de los costos de los controles de seguridad no puede estar por encima del valor de la información que necesita ser protegida.

Respecto a la administración de los riesgos, podemos citar cuatro opciones:

- ✓ Eliminación
- ✓ Mitigación
- ✓ Transferencia
- ✓ Aceptación o Financiación

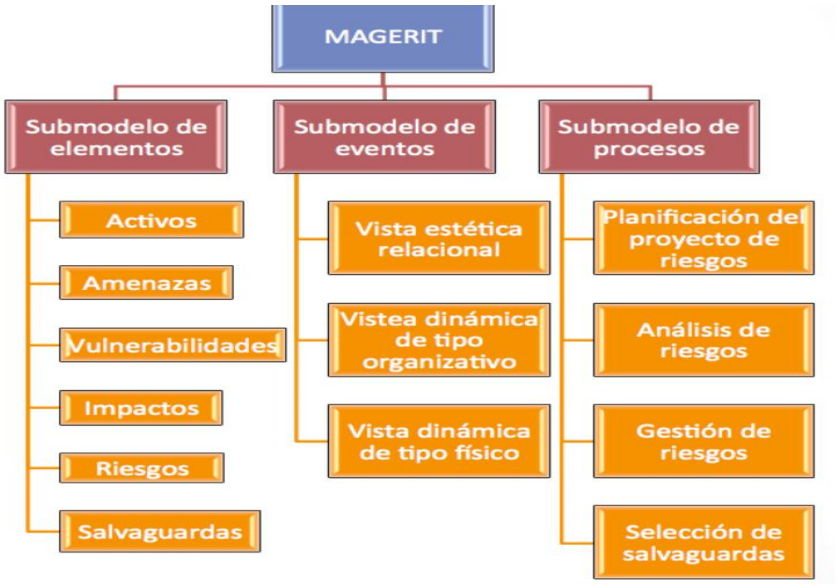
Dentro de la gestión de la seguridad informática y riesgo y control informático, es fundamental conocer y controlar los riesgos a los cuales está expuesta la información de la empresa, por lo regular estas siempre buscaran como implementar modelos de gestión de seguridad para esto suelen adoptar metodologías que brinden un marco de trabajo definido, que facilite la administración de los riesgos y de igual forma permita mejorarla.

Se determinó usar el MAGERIT ya que es una metodología de análisis y gestión de riesgos, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones permitiendo así implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados. Esta metodología también cuanta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos.

MAGERIT se basa en analizar el impacto que puede tener la empresa en la violación de la seguridad, buscando identificar las amenazas que pueda llegar afectar la empresa y las vulnerabilidades que pueden ser utilizadas por dichas amenazas, obteniendo un resultado final la identificación clara de las medidas preventivas y correctivas apropiadas que debe contar la entidad[35].

[35] GONZALEZ, DanielF. EL RIESGO Y LA FALTA DE POLITICAS DE SEGURIDAD INteoriFORMÁTICA UNA AMENAZA EN LAS EMPRESAS CERTIFICADAS BASC. Administración de la seguridad y salud Ocupacional. [en línea]. [citado el 2-06-17]. Disponible en http://repository.unimilitar.edu.co/bitstream/10654/12251/1/ENSAYO%20FINAL.pdf

Figura 1. Estructura de Magerit



Fuente: BOLAÑOS, María y GALVIS Mónica. Auditoria de si. MAGERIT v.3 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información). [En línea]. España: El autor, 2012. [Citado el 26-11-17]. Disponible en: https://asijav.weebly.com/auditoria-de-sistemas-de-informacioacuten/magerit-v3-metodologa-de-anlisis-y-gestin-de-riesgos-de-los-sistemas-de-informacin

Esta metodología contempla 3 libros:

- Método (Libro 1): Enumera los pasos y actividades para realizar un proyecto de análisis y gestión de riesgos, y proporciona una serie de aspectos prácticos.

- Catálogo de elementos (Libro 2). Clasifica los tipos de activos, dimensiones de valoración de los activos, criterios de valoración de los activos, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger sistemas de información en una organización.

- Guía de técnicas (Libro 3). Proporciona técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos.

2.1.6 Familia Normatividad ISO[36]

2.1.6.1 Normativa ISO 27000

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y

[36] [Citado el 26 de Noviembre de 2017].Disponible en: http://www.iso27000.es/iso27000.html

mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). La mayoría de estas normas se encuentran en preparación e incluyen: ISO/IEC 27000 - es un vocabulario estándar para el PSI. Introducción y base para el resto. Tercera versión: enero de 2014[37].

2.1.6.2 Normatividad ISO 27001

El 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados[38].

El principal objetivo de esta monografía en el Colegio Luis Carlos Galán Sarmiento, tiene como punto de partida la Norma ISO 27001, ya que está norma estudia la mejora continua en la gestión de seguridad, donde está planificada con el monitoreo, operación, seguimiento y revisión de cada proceso que se presente en la organización.

2.1.6.3 Normatividad ISO/IEC 27002

Publicada desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

Actualmente, la última edición de 2013 de este estándar ha sido actualizada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles publicándose inicialmente en inglés y en francés tras su acuerdo de publicación el 25 de Septiembre de 2013 [39].

---

[37] [Citado el 26 de Noviembre de 2017].Disponible en: https://es.wikipedia.org/wiki/ISO/IEC_27000-series

[38] [Citado el 26 de Noviembre de 2017].Disponible en: http://www.iso27000.es/iso27000.html

[39] [Citado el 26 de Noviembre de 2017].Disponible en: http://www.iso27000.es/iso27000.html

2.1.6.4 Normatividad ISO/IEC 27003

Publicada el 01 de Febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.

2.1.6.5 Normatividad ISO/IEC 27004

Publicada el 15 de Diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

2.1.6.6 Normatividad ISO/IEC 27005

Publicada en segunda edición el 1 de Junio de 2011 (primera edición del 15 de Junio de 2008). No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información.

2.1.6.7 Normatividad ISO/IEC 27006

Publicada en segunda edición el 1 de diciembre de 2011 (primera edición del 1 de Marzo de 2007) y revisada el 30 de Septiembre de 2015. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

2.1.6.8 Normatividad ISO/IEC 27007

Publicada el 14 de Noviembre de 2011. No certificable. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011. En España, esta norma no está traducida.

2.1.6.9 Normatividad ISO/IEC 27008

Publicada el 15 de Octubre de 2011. No certificable. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI. En España, esta norma no está traducida.

2.2 MARCO CONCEPTUAL

2.2.1 Políticas de Seguridad

Las políticas de seguridad informática tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes (Voz y Datos)) y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de cómputo de las empresas[40].

2.2.2 Norma ISO/IEC 27001:2013

La norma aquí mencionada es una solución basada en el ciclo de mejora continua o de Deming que se desarrolla en un SGSI para evaluar todo tipo de riesgo o amenazas, establecer controles y estrategias para minimizar peligros a los activos de una organización. Dicho ciclo conocido también como PHVA acrónimo de sus siglas: Planificar, Hacer, Verificar y Actuar.

Los pilares fundamentales que se basa el SGSI (Sistema de Gestión de Seguridad de la Información) para realizar los procesos de seguridad son:

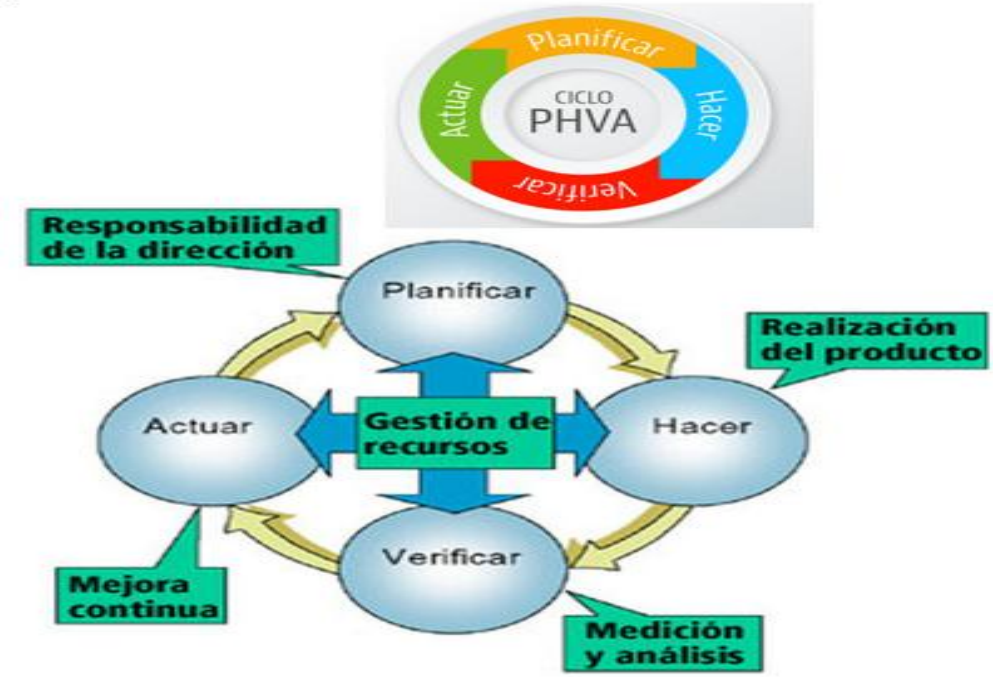
- ✓ Confidencialidad: es la garantía de acceso a la información de los usuarios que se encuentran autorizados para tal fin.
- ✓ Integridad: es la preservación de la información completa y exacta.
- ✓ Disponibilidad: es la garantía de que el usuario accede a la información que necesita en ese preciso momento.

Figura 2. Pilares fundamentales de SGSI

Fuente: BELT IBÉRICA. Seguridad informática. Objetivos de la seguridad informática, que tenemos que tener en cuenta? [En línea]. España: El autor, 2012. [Citado el 26-11-17]. Disponible en: http://azucenamarez.blogspot.com.co/2014_04_01_archive.html

[40] BENITEZ, Moisés. GESTION INTEGRAL: Políticas de Seguridad Informàtica.2013. [en línea]. [citado el 2-06-17]. Disponible en http://www.gestionintegral.com.co/wp-content/uploads/2013/05/Pol%C3%ADticas-de-Seguridad-Inform%C3%A1tica-2013-GI.pdf

Figura 3. Ciclo PHVA (Planificar, Hacer, Verificar y Actuar).



Fuente: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Ciclo PHVA. [Citado el 27-11-17]. Disponible en: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/12598/1/1097035128.pdf

El Sistema de Gestión de Seguridad de la Información tiene que tener en cuenta los tres pilares fundamentales para realizar el tratamiento de los riesgos de la organización ya que la implementación de los controles de seguridad son los activos de la organización[41].

2.3 ANTECEDENTES

- ✓ Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca; elaborado por John Jairo Perafán Ruiz y Mildred Caicedo Cuchimba; expone los riesgos que afectan a la información de la institución para dejar a un futuro la implementación de un sistema de seguridad mediante el análisis de riesgos[42].

[41] SOFTWARE DE GESTIÓN PARA LA EXCELENCIA EMPRESARIAL. Enero 13 de 2015. [en línea]. ISOTools. [citado el 2-06-17]. Disponible en: https://www.isotools.org/2015/01/13/iso-27001-pilares-fundamentales-sgsi/

[42] PERAFÁN , Jhon. Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. [en línea]. [citado en 27 de Noviembre de 2017]. Disponible en: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2655/3/76327474.pdf

La Institución Universitaria Colegio Mayor del Cauca, no tiene un sistema de seguridad de la información que permita la gestión de vulnerabilidades, riesgos y amenazas a las que normalmente se ve expuesta la información presente en cada uno de los procesos internos, no se tienen estandarizados controles que lleven a mitigar delitos informático o amenaza a los que están expuestos los datos comprometiendo la integridad, confidencialidad y disponibilidad de la información. Existen procedimientos creados subjetivamente por iniciativa y experiencia de los miembros del equipo TIC; por ejemplo, no existe una política de uso de claves de usuario, en los servidores se realiza el cambio de claves de acceso a criterio del personal responsable de cada uno de ellos sin una periodicidad y bitácora definida; los administrativos y docentes no hacen uso de claves de acceso, por lo que cualquier persona puede tener acceso a los equipos de cómputo que se les ha asignado. La Institución Universitaria tiene muchos inconvenientes dentro del manejo de la información debido a que ha ido creciendo paulatinamente y no se ha tomado conciencia de la importancia de asegurar la información existente; a medida que avanza es necesario adoptar y crear políticas que regulen las buenas prácticas en cada una de las transacciones, procesos y recursos relacionados con la información y para esto, es indispensable realizar el análisis de riesgos de la seguridad de la información, incluyendo los activos que directa e indirectamente están ligados a este proceso, como lo dicta la metodología Magerit. De no integrar dentro de sus sistemas, buenas prácticas y recomendaciones de seguridad informática, resultado del análisis de riesgos; muy seguramente en un futuro cercano podría ser víctima de delitos informáticos que obstaculicen su normal funcionamiento como lo pueden ser intrusiones, modificación y/o robo de información, denegación de servicios, entre otros.

- ✓ Instituto Colombiano De Crédito Educativo Y Estudios Técnicos En El Exterior Manual De Políticas De Seguridad De La Información; donde el documento describe las políticas y normas de seguridad de información con el fin de regular la gestión de seguridad de la información al interior de la entidad[43].

- ✓ El Riesgo Y La Falta De Políticas De Seguridad Informática Una Amenaza En Las Empresas Certificadas Basc. Autores: Daniel Felipe González Agudelo.

El presente ensayo está enfocado en el numeral 7 de los estándares de seguridad de la norma BASC, el cual menciona la seguridad en las tecnologías de la información (protección con contraseñas, responsabilidad y protección a los sistemas y datos). El tema a desarrollar se enfoca en la problemática que conlleva no tener políticas, procedimientos y/o normas de seguridad informática en las empresas certificadas BASC. La protección de datos, documentos y control de acceso a la información es un tema que cada día toma más fuerza en las grandes compañías, debido a las diferentes especialidades de hackers y crackers que roban información vital.

[43] ICETEX. Instituto Colombiano De Crédito Educativo Y Estudios Técnicos En El Exterior Manual De Políticas De Seguridad De La Información. [en línea]. [citado en 27 de Noviembre de 2017]. Disponible en: https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manualseguridadinformacion.pdf

Los elementos de la información son denominados los activos de una institución los cuales deben ser protegidos para evitar su perdida, modificación o el uso inadecuado de su contenido.

Generalmente se dividen en tres grupos:

- ✓ Datos e Información: Son los datos e informaciones en sí mismo
- ✓ Sistemas e Infraestructura: Son los componentes donde se mantienen o guardan los datos e informaciones
- ✓ Personal: Son todos los individuos que manejan o tienen acceso a los datos e informaciones y son los activos más difíciles de proteger, porque son móviles, pueden cambiar su afiliación y son impredecibles.

No tener una política de seguridad de la información clara y definida, lleva inevitablemente al acceso no autorizado a una red informática o a los equipos que en ella se encuentran y puede ocasionar en la gran mayoría de los casos graves problemas. El principal riesgo es el robo de información sensible y confidencial, el cual puede ocasionar hasta el cierre de una compañía solida financieramente.

La pérdida o mal uso de información confidencial genera daños y repercusiones relacionados con la confidencialidad, integridad y disponibilidad de los archivos para las empresas y a su vez para el titular del documento. La seguridad informática se distingue por tener dos propósitos de seguridad, la Seguridad de la Información y la Protección de Datos, estos se diferencian debido a que los datos son valores numéricos que soportan la información mientras que la información es aquello que tiene un significado para nosotros. En ambos casos las medidas de protección aplicadas serán las mismas.
Palabras clave: Seguridad Informática, protección de datos, hackers, crackers, elementos de la información.

- ✓ Diseño de políticas de seguridad informática basadas en la norma ntc-iso-iec 27001:2013 para la universidad de Cartagena centro tutorial Mompox Bolívar; elaborado por Manuel Esteban Ureche Ospino; el propósito del proyecto es proporcionar y garantizar la seguridad de la información de los recursos informáticos de la Universidad de Cartagena Centro Tutorial Mompox, mediante políticas de seguridad informática.

El presente trabajo de grado tiene como propósito diseñar las políticas de seguridad informática para Universidad de Cartagena Centro Tutorial Mompox, Teniendo en cuenta el análisis de riesgos y vulnerabilidades, tomando como referencia la norma NTC-ISO-IEC 27001:2013, es por ello que en este proyecto se platea el diseño de las políticas de seguridad informática. El propósito de este proyecto es proporcionar y garantizar la seguridad de la información de los recursos informáticos de la Universidad de Cartagena Centro Tutorial Mompox.

El proyecto se apoya en estudios realizados a los estudiantes de la Universidad de Cartagena Centro Tutorial Mompox y personal administrativo, donde se desarrollaron varias entrevistas al personal que administra el área de sistemas y recursos informáticos, de acuerdo a la información levantada se tomó una muestra de acuerdo a las necesidades de seguridad, utilizando estadística no probabilística donde se evidencia que no existen políticas de seguridad informática que se apliquen para este centro tutorial.

De acuerdo a lo anterior es importante destacar que la seguridad de la información y las políticas de seguridad informática tiene un papel importante en cualquier Universidad de estudios superior en el país, por ello es importante desarrollar las mejores prácticas de seguridad, con el fin de mantener un alto nivel de protección de la información.

Palabras claves: Seguridad informática, instituciones de educación superior, políticas, vulnerabilidades, amenazas, riesgo, norma NTC-ISO-IEC 27001:2013[44].

Sistema de información para la Administración de un colegio; elaborado por Paolo López Rengifo; expone Análisis, diseño, desarrollo e implementación de un Sistema de Información para la Administración de los procesos básicos de un colegio.

Alcances:

- ✓ Educación Básica Regular.
- ✓ Niveles de Primaria y Secundaria.
- ✓ Periodos de evaluaciones bimestrales.
- ✓ Turnos de mañana y tarde.
- ✓ Días de clase de lunes a viernes o lunes a sábado.
- ✓ Recaudación de pagos para las obligaciones de los alumnos a través de una o más entidades bancarias.

Funcionalidades:

- ✓ Procesos básicos de colegio desarrollados:
- ✓ Elaboración y cálculo de notas.
- ✓ Control en las asistencias de los profesores.
- ✓ Control en las asistencias de los alumnos.
- ✓ Seguimiento a las obligaciones de pago en los alumnos.
- ✓ Seguridad en el uso del sistema a nivel de menú y acciones.
- ✓ Modo de trabajo Multiusuario.
- ✓ Criterios técnicos:

[44] URECHE, Manuel. Diseño de políticas de seguridad informática basadas en la norma ntc-iso-iec 27001:2013 para la universidad de Cartagena centro tutorial mompox bolívar. Universidad nacional abierta y a distancia unad especialización en seguridad informática. [en línea]. [citado en 27 de Noviembre de 2017]. Disponible en: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/12027/1/19772159.pdf

- ✓ Implementación en arquitectura 3 capas.
- ✓ Implementación en plataforma Web.
- ✓ Empleo de tecnología Java como lenguaje de desarrollo.
- ✓ Utilización de PostgreSQL como motor de base de datos.
- ✓ Utilización de una metodología orientada a objetos.
- ✓ Utilización de la notación UML.

El trabajo expuesto ofrece servicios que pretenden en comparación al trabajo tradicional reducir los tiempos ineficientes, integrar datos y obtener una mejor información. Asimismo, el empleo de la Web como medio tecnológicamente de vanguardia en cuanto a su uso para la Internet, y el de herramientas y tecnologías libres que brindan una respuesta al propósito de disminuir los costos por concepto de adquisición de licencias en beneficio de que los colegios puedan adquirir un aplicativo a un precio que les sea accesible, se añaden entre sus principales beneficios.

2.4 MARCO LEGAL

2.4.1 Ley Estatutaria 1266

"Por la cual se dictan las disposiciones generales del hábeas data 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" [45].

2.4.2 Decreto 1360 de 1989

"Donde se reglamenta el soporte lógico (software) en el registro nacional de derecho de autor, considerando al software como una creación del dominio literario en conformidad a la ley 23 de 1982 sobre derechos de autor[46].

2.4.3 Ley 57 de 5 de junio de 1985

"Por la cual se ordena la publicidad de los actos y documentos oficiales"[47].

2.4.4 Ley 527 de 18 de Agosto de 1999

[45] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (Diciembre 31 de 2008). Diario Oficial 47.219 de diciembre 31 de 2008. p. 1-15.

[46] JARAMILLO, A. Manual de derecho de autor. (en línea). (7 de Junio de 2017). Disponible en: http://www.derechodeautor.gov.co/documents/10181/331998/Cartilla+derecho+de+autor

[47] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 57 de 1985 (julio 5 de 1985). Bogotá. Diario Oficial 05 de julio de 1985. p. 1-6.

"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"[48].

2.4.5 Ley 1273 de 2009

"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"[49]

2.4.6 Decreto 1747 de 2000

"Que reglamenta parcialmente la ley 527 de 1999, con lo relacionado a las entidades de certificación, los certificados y las firmas digitales"[50].

2.4.7 Decreto 1727 de 15 de mayo de 2009

"Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información"[51].

2.4.8 Resolución 26930 de 2000

"La cual fija los estándares para la autorización y el funcionamiento de las entidades de certificación y sus auditores"[52].

2.4.9 Ley 1273 de 2009

"con la que se modifica el código penal, se crea un nuevo bien jurídico denominado "de la protección de la información y los datos", y se preservan

---

[48] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527 (18 de agosto de 1999). Bogotá. Diario Oficial 43.673 de 21 de agosto de 1999. p 1-2.

[49] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (05 de enero de 2009). Bogotá. Diario Oficial 47.223 de enero 5 de 2009. p. 1-15.

[50] Decreto. Artículo 160 del Decreto ley 19 de 2012. (en línea). (7 de junio de 2017). Disponible en: http://www.sic.gov.co/propiedad-Industrial

[51] COLOMBIA. CONGRESO DE LA REPÚBLICA. Decreto 1727 (15 de mayo de 2009). Bogotá. Diario Oficial 47.350 de mayo 15 de 2009. p. 1-5.

[52] Resolución. Por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores. (en línea). (7 de junio de 2017). Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5793

integralmente los sistemas que utilicen las tecnologías de información y de comunicación"[53].

2.4.10 Ley Estatutaria 1266 del 31 de diciembre de 2008

"Por la cual se dictan las disposiciones generales del hábeas data 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"[54].

2.4.11 Decreto 1377 de 2013

"Por el cual se reglamenta parcialmente la Ley 1581 de 2012"[55].

2.4.12 Ley 1341 de 2009

"Por la cual se definen 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 de Espectro y se dictan otras disposiciones"[56]

2.4.13 Ley Estatutaria 1581 de 2012

"Por la cual se dictan disposiciones generales para la protección de datos personales"[57]

2.4.14 Ley nacional:

La Constitución de 1991, La Ley General de Educación 115 de 1994 y el decreto 1860/94 establecen las normas de la administración y organización del sistema educativo en Colombia. De acuerdo con estas la comunidad educativa participara en la dirección de los establecimientos educativos, en los términos de la ley. La comunidad educativa estará conformada por estudiantes, educadores, padres de familia o acudientes, egresados, directivos docentes y administradores escolares. Todos ellos, según su competencia, participaran en el diseño. Ejecución y evaluación del Proyecto educativo Institucional y en la buena marcha del respectivo establecimiento educativo[58].

---

[53] DELTA. (2014). Ley de delitos informáticos en Colombia. (en línea). (7 de junio de 2017). Disponible en: http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

[54] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1266 (diciembre 31 de 2008 Bogotá. Diario Oficial 47.219 de 31 de diciembre de 2008. p. 1-19.

[55] COLOMBIA. CONGRESO DE LA REPÚBLICA. Decreto 1377 (27 de junio de 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Diario Oficial 48.834 de 27 de junio de 2013. p. 1-11.

[56] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1266 (julio 30 de 2009). Bogotá. Diario Oficial 47.426 de julio 30 de 2009. p. 1-34.

[57] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1581 (octubre 17 de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial 48.587 de octubre 18 de 2012. p. 1-15.

[58] Ministerio de educación nacional. Decreto 1860 de 1994. (1994). (en línea). (27 de Noviembre de 2017). Disponible en: http://www.mineducacion.gov.co/1621/articles-172061_archivo_pdf_decreto1860_94.pdf

3. VERIFICAR LA SITUACIÓN ACTUAL DE LA INSTITUCIÓN EDUCATIVA LUIS CARLOS GALÁN SARMIENTO

Se hace necesario realizar una verificación de la información de los activos y de la estructura organizacional con que cuenta el Colegio Luis Carlos Galán Sarmiento para diagnosticar la situación del área de sistemas, infraestructura y servicios que presta en cada una las secciones administrativas y académicas; así de ésta manera, conocer la situación de la institución para el análisis y gestión de riesgo con la metodología Magerit v3, libro 2.

3.1 DESCRIPCION DEL COLEGIO

Dentro del marco del PEI Galanista que considera la educación como "un proceso de investigación y construcción del proyecto de vida", con base en los ejes de participación y representación, formulados por la Constitución Política de Colombia; y teniendo en cuenta las políticas educativas de orden nacional y distrital, los roles y características propias de los diferentes actores responsables y las condiciones socioeconómicas, culturales, políticas y democráticas de la comunidad educativa, formuló y adoptó el horizonte institucional.

3.1.1 Historia

La Institución Educativa "Luis Carlos galán sarmiento", fue creada el 20 de Enero de 1989 con el nombre de Colegio Distrital La Ponderosa y por acuerdo Nº 15 del 28 de Noviembre del mismo año, emitido por el consejo de Bogotá, se cambia su nombre por COLEGIO DISTRITAL LUIS CARLOS GALAN SARMIENTO, como homenaje al líder político.[59]

3.1.2 Misión

Ofrecer una educación de calidad centrada en el desarrollo integral humano, a través de aprendizajes que impliquen la apropiación y vivencia de principios, valores, saberes y competencias, que coadyuven al cambio, la transformación personal, familiar y social[60].

3.1.3 Visión

Hacia el año 2020 el Colegio Distrital Luis Carlos Galán Sarmiento I.E.D., será reconocido como una institución competente en la formación de ciudadanos responsables, conscientes y comprometidos con el cambio social, el desarrollo sostenible y el respeto por los derechos humanos; mediantes la construcción de

---

[59] Colegio Luis Carlos Galan Sarmiento. Proyecto de Vida Galanista. Recuperado de: http://www.colegioluiscarlosgalansarmiento.edu.co/index.php?lang=es

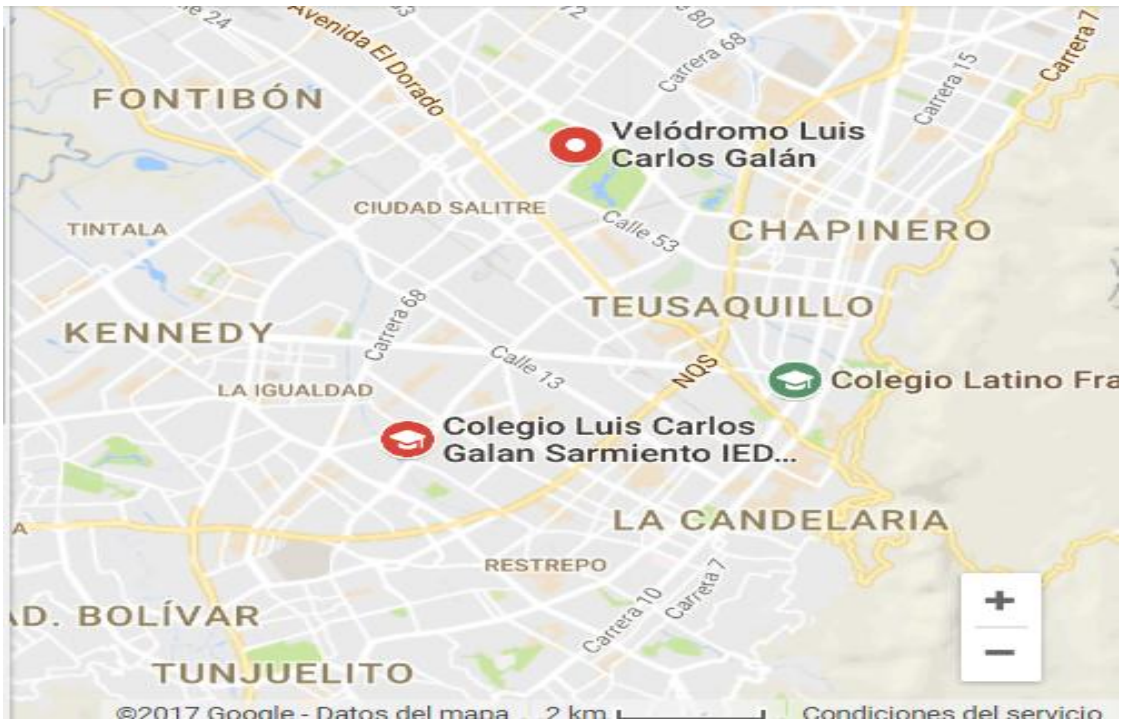
[60] Colegio Luis Carlos Galan Sarmiento. Proyecto de Vida Galanista. Recuperado de: http://www.colegioluiscarlosgalansarmiento.edu.co/index.php?lang=es

proyectos de vida que den respuesta a las necesidades y expectativas presentes y futuras.

3.1.4 Ubicación geográfica

La institución se encuentra ubicada en Calle 1B # 52A-02, PUENTE ARANDA, una zona Industrial y Residencial. El 90% de la población estudiantil proviene de hogares o familias clasificadas en estrato tres, aunque se presenta el fenómeno de los inquilinatos. Se observa un alto impacto industrial especialmente por los grados de contaminación ambiental que esta actividad genera; un amplio número de los habitantes desarrollan actividades de tipo comercial independiente alrededor de los San Andresitos, adquiriendo una connotación de informalidad y de subempleo, en la actualidad se observa un alto índice de desempleo y empobrecimiento aunque la mayoría de su población está clasificada como clase media- media.

Figura 4. Ubicación geográfica CLCGS



Fuente: Google Maps. [en línea]. [Citado el 27-11-17]. Disponible en https://www.google.com.co/maps/@4.6111652,-74.1225903,19z

3.1.5 Objetivos estratégicos de la institución para lograr la misión y visión

- ✓ Fortalecer los desempeños académicos, mediante la implementación de estrategias pedagógicas didácticas que aseguren la apropiación y alcance de los aprendizajes propuestos.

- ✓ Fortalecer el perfil ético, convivencial y social del estudiante Galanista de acuerdo con el marco de principios y valores institucionales propuestos en e PEI.

- ✓ Implementar y ajustar acciones pedagógicas a los planes, programas y proyectos de orden nacional, distrital y local, que se requieran para su aplicación en la institución, hacia el alcance de una educación integral y de calidad.

3.1.6 Principios Institucionales

Tabla 1. Principios Institucionales

PRINCIPIOS INSTITUCIONALES	
PRINCIPIOS	**VALORES**
Proyección y Cambio	Autonomía - Autoestima - Liderazgo - Orden y aseo - Racionalización de Recursos
Participación y compromiso	Liderazgo - Aptitudes - Autodisciplina - Trabajo en Equipo
Ser social y ser ciudadano	Lealtad - Amor - Paz - Paciencia - Tolerancia - Justicia - Honestidad - Libertad Solidaridad - Respeto - Sentido de pertenencia - Amor a la familia y a la patria.
Formación afectiva, cognitiva y expresiva	Sabiduría - Superación - Creatividad - Iniciativa - Responsabilidad - Adaptabilidad Autocrítica - Capacidad de comunicación

Fuente: Manual de Convivencia del Colegio Luis Carlos Galán. [en línea]. [Citado el 27-07-17]. Disponible en https://es.calameo.com/read/00319224995f440b9a48a

3.1.7 Enfoque pedagógico Galanista

El enfoque pedagógico Galanista, está orientado hacia el desarrollo del estudiante como ser humano integral, desde sus aprendizajes, la práctica de valores, la iniciativa individual, la creatividad y el ejercicio de la ciudadanía y la convivencia pacífica.
Este enfoque con lleva a la formación de un estudiante integral que interactúa para el cambio y la transformación social. Está orientado hacia el desarrollo de las dimensiones del ser humano: actitudinal (ser), cognitivo (saber) y procedimental (saber hacer). Desde el ser, promovido en formación en los principios y valores sociales tales como autonomía, respeto, trabajo en equipo,

responsabilidad y liderazgo entre otros; que le permiten reconocerse y ser reconocido como ciudadano de bien en los diferentes escenarios de la vida. Desde el saber, promoviendo la construcción y apropiación de aprendizaje que le permite ser competente en diferentes escenarios escolares, académicos y profesionales. Desde el saber hacer, promoviendo la interacción con su contesto desde la dinámica del aprendizaje continuo, el liderazgo, la proyección, el cambio, el compromiso social y ambiental.

3.1.8 Horizonte Galanista para el desarrollo Humano

El horizonte Galanista está dado por todas las dimensiones integrales de un ser humano como transformador de la sociedad, teniendo en cuenta todos los valores, ética, moral y aprendizajes hacia el bienestar común.

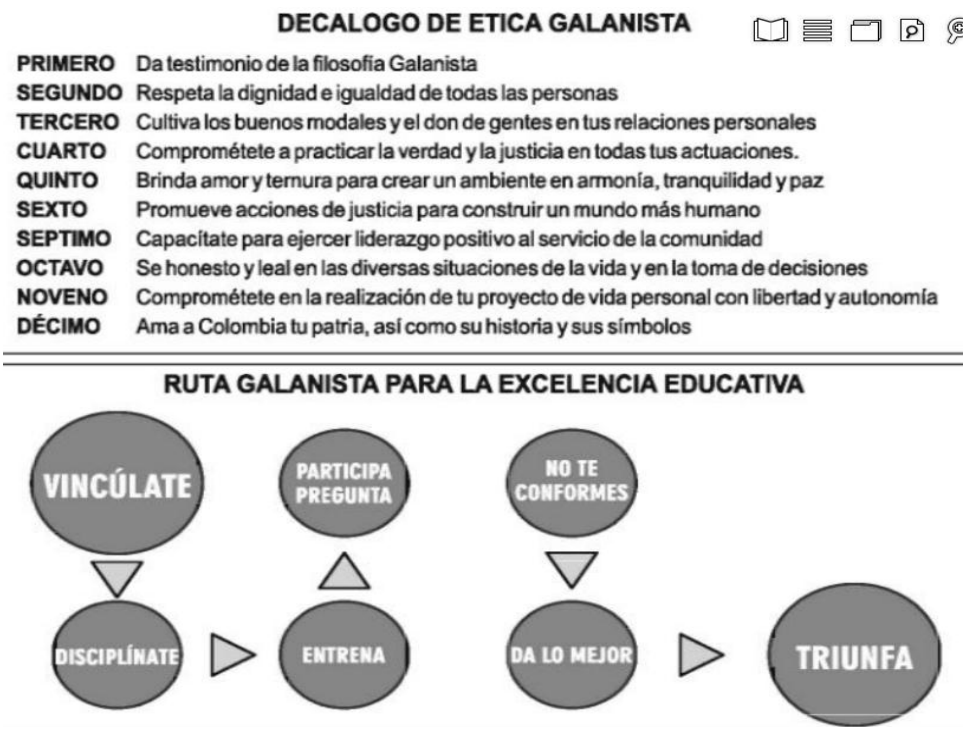
Figura 5. Horizonte Galanista

Fuente: Manual de Convivencia del Colegio Luis Carlos Galán. [en línea]. [Citado el 27-07-17]. Disponible en https://es.calameo.com/read/00319224995f440b9a48a

3.1.9 Perfil Galanista Estudiante

El estudiante Galanista es una persona con grandes potenciales, capaz de transformar y trascender con la cooperación de toda la comunidad educativa; asumiendo una actitud analítica, critica, reflexiva, participativa e interactiva frente a los diversos sucesos locales, nacionales e internacionales. Es el agente que imprime junto con su maestro dinamismo, relevancia y pertinencia al acto educativo.

Tabla 2. Decálogo de ética Galanista



Fuente: Manual de Convivencia del Colegio Luis Carlos Galán. [en línea]. [Citado el 27-07-17]. Disponible en https://es.calameo.com/read/00319224995f440b9a48a

3.1.10 Tras las huellas del colegio Luis Carlos Galán Sarmiento

El Colegio Luis Carlos Galan Sarmiento, IED, ha asumido con responsabilidad el compromiso de trabajar por la calidad educativa de la educación, no solo en Bogotá, sino ante el país. En ese largo camino desde 1981, por otra Escuela Distrital “La Ponderosa”, hasta nuestros días, nos ha marcado siempre el sello de querer hacer las cosas bien desde la primera vez. Para ello es necesario, planear, verificar, hacer, actuar, como un modelo de gestión institucional enmarcado en cada uno de sus procesos educativos y administrativos.

Somos un “colegio de páginas abiertas” es decir, para que nos lean, nos miren y a su vez, nosotros, tengamos la oportunidad de aprender de otros. De tal modo que cuando hablamos de procesos exitosos, estos han sido construidos de manera colectiva, participativa, armoniosa, erigidos por un Decálogo Galanista del que satisfactoriamente dan cuenta nuestros egresados. Por eso afirmamos que somos institución de calidad: porque nada se improvisa, hay un horizonte institucional, unos objetivos estratégicos, y los resultados nos permiten sentirnos orgullosos, como comunidad, de lo alcanzado en una visión proyectada hacia el 2020.

Galardón de la Excelencia (2004-2005), distinciones del sector público y privado, la sostenibilidad de las Pruebas Saber, la Educación Media Fortalecida y el acceso a la Educación Superior, Ser Pilo Paga, docentes beneficiados con estudios de postgrado apoyados por la SED y con producciones de experiencias de aula, vinculaciones de valiosa ayuda con la Cámara de Comercio de Bogotá, el reconocimiento a directivos y docentes por el posicionamiento de la institución en el ámbito de los colegios públicos del Distrito Capital, al igual que los trofeos obtenidos en los Juegos Intercolegiados y el Premio y Reconocimiento a la INCITAR de la institución - proyecto de la SED -, como una de las mejores de la capital colombiana, son algunas de las menciones destacadas que ha recibido el Colegio Luis Carlos Galán Sarmiento para la localidad 16 de Puente Aranda y para Bogotá. Cabe resaltar también, el Premio Nacional, Bolsa Millonaria, de la Bolsa de Valores, obtenido por el estudiante Daniel Beltrán en el grado 10, acreditado en dinero y en futura beca en la Universidad de La Sabana.

Estas huellas han sido orientadas desde que nació la institución por su rectora, Stella Reyes de Lemus, con equipos de maestros, estudiantes, padres de familia, estamentos administrativo, todos abnegados, visionarios, convencidos de lo que dice Mandela, y de que si impulsamos, desarrollamos y promovemos una educación de calidad, de alguna manera, estamos contribuyendo para que Colombia sea la mejor educada de la región en el 2025. Ese camino lo conducen los principios y valores institucionales, nuestros proyectos transversales, el entusiasmo de todos los miembros de la comunidad educativa, el convencimiento de que la paz es el camino para mejorar la calidad de vida de los pueblos, y por supuesto, nuestro faro también son las metas que día a día nos proponemos para deja huella en la educación bogotana. Sigamos haciendo historia, Luis Carlos Galán Sarmiento.[61]

3.2 ESTRUCTURA ORGANIZACIONAL

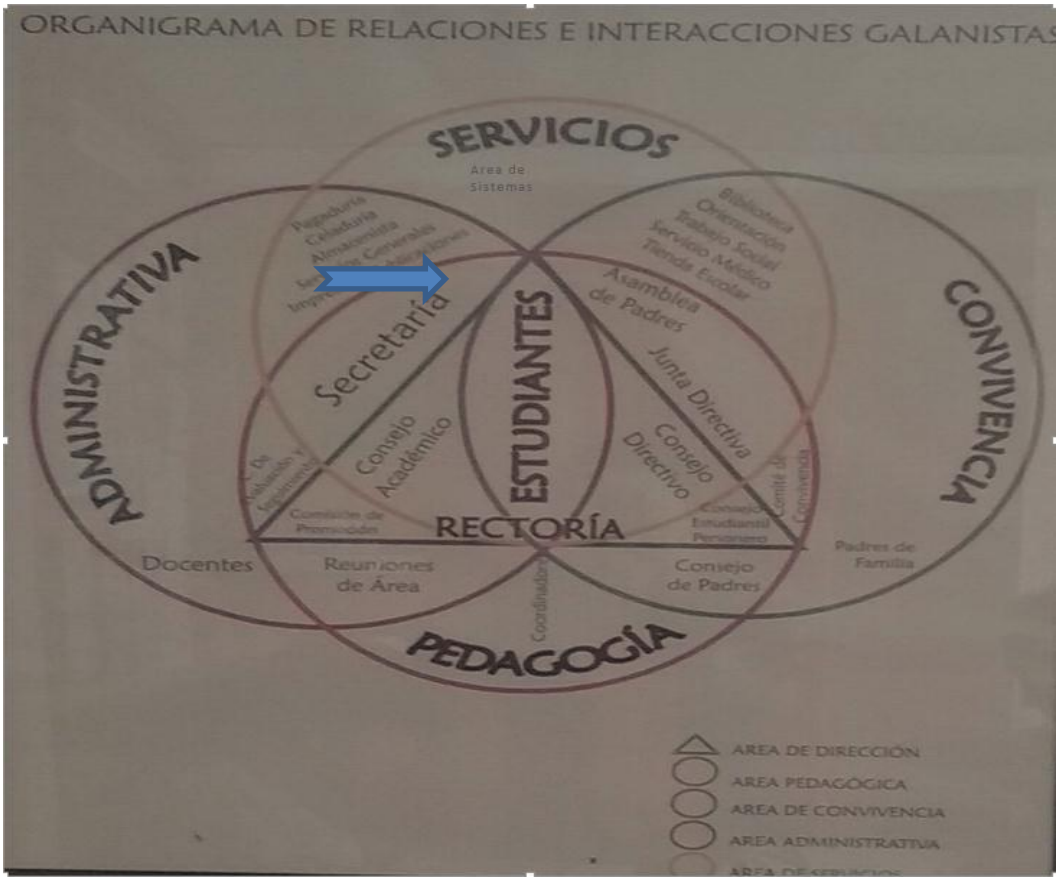
La estructura organizacional da como elemento central al Gobierno Escolar, el cual proyecta acompañamiento, orientación, asesoría y apoyo a los cuatro componentes como son: Administrativa, Pedagógica, Convivencial y de servicios. Este sistema central se realimenta de las áreas periféricas, proyectadas a la formación integral del estudiante. La rectoría transciende la gestión de manera estratégica a los cuatros componentes para la sostenibilidad, innovación, proyección y mejoramiento continuo. El Consejo Directivo está considerado como un organismo de apoyo y participación. El consejo académico define y orienta acciones pedagógicas y convivenciales. Esta organización sistemática, facilita la comunicación efectiva, participación, delegación y toma de decisiones, puesto que cada una tiene sus propias funciones y desarrollan procesos que aunque tienen puntos comunes, ejercen autonomía en las prácticas y responsabilidad del día a día.

[61] Montealegre A. (2017). *Tras las huellas del Colegio Luis Carlos Galán Sarmiento*.

En el proceso clave y responsable del organismo del Colegio Luis Carlos Galán Sarmiento, en cabeza de la Señora Rectora, está dado por proceso pedagógico encargado por Consejo Académico y coordinadores; el proceso Convivencial encargado por Comité de Convivencia y coordinador; El proceso financiero por el Área Contable y Auxiliar Financiero; el proceso Administrativo por el organismo Secretaria – Almacén y proceso de Servicios por el organismo Biblioteca, Orientación, Administrador Tienda Escolar, Ludoteca, Compañía Privada (Vigilancia y servicio de Aseo).

Para asegurar la medicación y comprensión del direccionamiento estratégico y sus respectivo ajustes, la Dirección de la IED despliega los contenidos y asigna las responsabilidades, a través de la creación de espacios de formales tales como reuniones, asambleas, talleres y encuentros con los diferentes estamentos de la comunidad.[62]

Figura 6. Organigrama de Relaciones Galanistas



Fuente: Fotografía, Colegio Luis Carlos Galán Sarmiento

[62] P.E.I. Manual de Convivencia. [en línea] [citado el 27-09-2017]. Disponible en: http://es.calameo.com/read/00319224921eace6c3e85

3.3 AREA DE SISTEMAS

El Colegio Luis Carlos Galán Sarmiento Tiene Cinco (5) Ingenieros de Sistemas, docente, en el área de Media Integrada y dos (2) licenciados en Informática; encargados del buen funcionamiento del área de sistemas. Los docentes de Jornada mañana y Jornada Tarde, 55 profesores, también tiene acceso a utilizar los sistemas informáticos para complementar sus labores académicas. La institución cuenta con dos (2) sala de informática y una parte administrativa que son los que principalmente manipulan la información y los sistemas informáticos.

3.3.1.1 CARACTERIZACION DEL AREA DE SISTEMAS

El colegio Luis Carlos Sarmiento cuenta con:

- ✓ 12 Access point distribuidos en todo el colegio (Primaria - Secundaria).
- ✓ 2 Salas de Sistemas con 36 computadores cada una
- ✓ 72 antenas wifi para Pcs, se encuentran en las 2 salas de tecnología.
- ✓ 1 Sala de Orientación con dos computadores
- ✓ Una sala de Bilingüismo con 25 portátiles y 8 computadores de mesa
- ✓ Área 5 en 1 con 5 computadores(2 antenas wifi para PC y 3 computadores cableados)
- ✓ 1 laboratorio de Química con 35 portátiles
- ✓ Oficina de Rectoría con 1 computador
- ✓ Oficina Almacén, 1 computador
- ✓ Oficina Pagaduría , 1 computador
- ✓ 1 Oficina de Coordinación con 3 computadores y una impresora inalámbrica
- ✓ Sala de Ludoteca con 3 computadores de mesa.
- ✓ 1 Sala de Biblioteca con 5 computadores de mesa y 2 impresoras multifuncional
- ✓ 22 Tablets
- ✓ 1 Oficina de orientación con 1 computador de mesa.
- ✓ Cuenta con 1 Tablero Wifi
- ✓ 1 Rack
- ✓ 1 Cisco 2900 series (Router para dar servicio a empresas medio).
- ✓ 4 Switch

Tabla 3. Área de Sistemas CLCGS

	Portátiles	PC	Ubicación	Descripción	Sede	Conexión	Acces Poir
		36	Sala 1	Rack - Tablero	Bachillerat	Cable	1
		36	Sala 2	Impresora	Bachillerat	Wifi	1
		2	Orientación		Bachillerat	Wifi	1
	25	8	Bilingüismo		Bachillerat	Wifi	1
		5	5 en 1		Bachillerat	Cable	1
		1	Lab. Física		Bachillerat	Wifi	1
	35		Lab. Química		Bachillerat	Wifi	1
		1	Rectoría		Bachillerat	Wifi	
		1	Almacén		Bachillerat	Wifi	1
		1	Pagaduría		Bachillerat	Wifi	1
		3	Coordinación	Impresora inala	Bachillerat	Wifi	1
		5	Biblioteca	2 Impresoras	Bachillerat	Wifi	
		1	Orientación	Impresora	Bachillerat	Wifi	1
	35	3	Ludoteca	Impresora	Primaria	Wifi	1
Totales	95	103					12

Fuente: Propiedad de los autores

3.3.1.2 Misión

Proyectar, desarrollar, construir y conservar servicio de tecnología de información (TI), que contribuyan a la eficiencia de los procesos administrativos, académicos y de investigación.

3.3.1.3 Objetivos

- ✓ Interpretar y desarrollar el conocimiento Lógico para entender los procesos que intervienen en el campo de la Informática y la Tecnología.
- ✓ Desarrollar metodologías para la solución de problemas a partir de la construcción de algoritmos.
- ✓ Interpretar algoritmos y traducirlos al lenguaje de máquina.
- ✓ Fomentar en el estudiante la destreza en la aplicación de algoritmos computacionales orientados a la solución de problemas.
- ✓ Fortalecer habilidades de pensamiento de orden matemático y computacional.
- ✓ Dar a conocer los diversos elementos que intervienen en las redes de comunicaciones
- ✓ Observar las nociones de las redes de comunicaciones y sus implicaciones en el mundo global.
- ✓ Analizar el funcionamiento de las redes computacionales y sus ventajas en el ámbito empresarial.
- ✓ Detectar fallas y encontrar soluciones en el ensamble y montaje de redes computacionales.
- ✓ Reconocer los elementos internos y externos de los sistemas operativos.

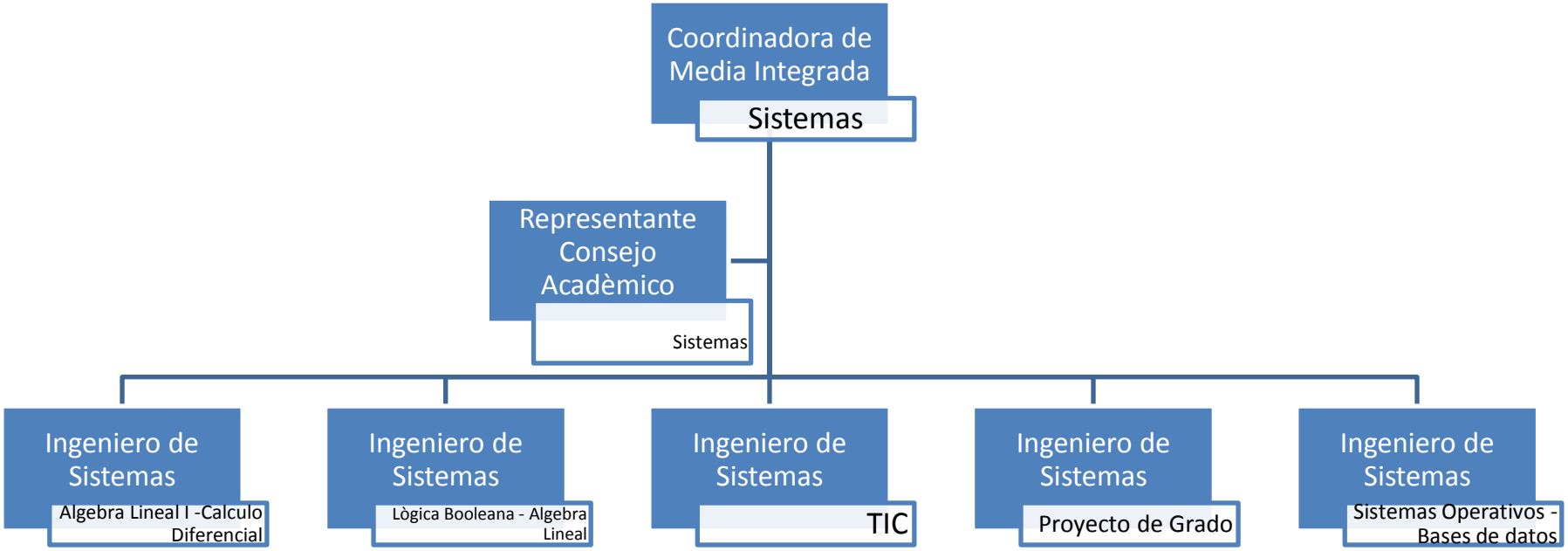
- ✓ Reconocer la administración y gestión de los sistemas operativos en los componentes tecnológicos.
- ✓ Configurar y analizar el funcionamiento de los sistemas operativos y dar soluciones acertadas en los fallos y daños detectados en el SO.
- ✓ Almacenar información de los estudiantes, docentes y de todos los activos de la institución.

3.3.1.4 Estructura Organizacional del área de sistemas

La estructura organizacional en el área de sistema está compuesta de la siguiente manera a saber:

- ✓ Coordinadora de Media Integrada
- ✓ Representante al consejo académico
- ✓ 5 docentes de media integrada.

Figura 7. Estructura Organizacional



Fuente: Propiedad de los autores

3.3.1.5 Descripción de cargos y funciones

Cada Syllabus institucional del área de sistemas está compuesto por presentación de la asignatura y una descripción de los fines educativos.

- ✓ Lógica Boolena: La Lógica y Algebra Booleana es una materia teórica que incluye la elaboración de unos ejercicios prácticos que dan a conocer todos los elementos necesarios para utilizar técnicas algebraicas y llevarlas a lógica proposicional mediante Álgebra de Boole, es un proceso de simbología que ayuda a comprender sucesos de la realidad y los lleva a comprimir en pequeñas escrituras o programas, utilizando sentencias y estrategias de lógica y Sinéctica. La ayuda tecnológica que utiliza el docente en su área es: Metodología basada en el trabajo colaborativo que parte de un espacio virtual, diseñado por el profesor y de acceso restringido, en el que se pueden compartir documentos, trabajar sobre ellos de manera simultánea, agregar otros nuevos, comunicarse de manera síncrona y asíncrona, y participar en todos los debates que cada miembro puede constituir. (Plataforma Moodle mflcgs.gnomio.com).

- ✓ Cálculo diferencial: El Cálculo Diferencial le proporciona al estudiante los fundamentos matemáticos necesarios para apropiarse de los conceptos básicos en su formación como ingeniero y le permite construir procesos sistemáticos y analíticos que desarrollen el pensamiento científico. A la vez propicia el desarrollo de habilidades de razonamiento lógico que facilitan el aprendizaje de conocimientos matemáticos que requieren mayores niveles de abstracción; contando con la ayuda tecnológica: Aplicación Geogebra.

- ✓ Proyecto de grado: Formular y gestionar proyectos tecnológicos a partir de un enfoque ingenieril visto desde la definición del problema o necesidad, el análisis, el diseño, la validación y la sustentación de propuestas o alternativas de solución a problemáticas que afecten de manera significativa el entorno; con ayuda tecnológica: Paquete de Office e Internet.

- ✓ Bases de datos: Con este curso se espera que el estudiante se apropie de conceptos y fundamentos teóricos básicos sobre la evolución, fundamentos, sistemas gestores de bases de datos, futuro de las bases de datos, modelado de sistemas orientado a bases de datos, modelo entidad relación, modelo relacional, diccionario de datos.

Los objetivos que el estudiante deberá alcanzar al finalizar el curso Bases de datos son los siguientes:

- Identificar la terminología propia de la bases de datos.
- Comprender los diferentes modelos de bases de datos, y en concreto dominar el modelo relacional.

- Ser capaz de realizar el modelo de una base de datos relacional, a partir de la especificación de requerimientos de un proyecto, comprendiendo y aplicando los conceptos y transformaciones implicados.

Conocer el uso y administración de dos de los gestores de bases de datos relacionales más populares en el ámbito del software libre

- ✓ Algebra Lineal: Algebra Lineal I es una asignatura disciplinar de formación en matemáticas que brinda conceptos y aplicaciones fundamentales de matrices, sistemas de ecuaciones lineales y determinantes. El manejo de Matrices y determinantes es el eje central de esta asignatura, en la cual se trata los diferentes temas asignados dentro del curso que permite dar soporte a otras herramientas de búsqueda de soluciones de ecuaciones y problemas diarios. Los software a utilizaroftware (MatLab – Derive wólfram Alfa - Geogebra) .

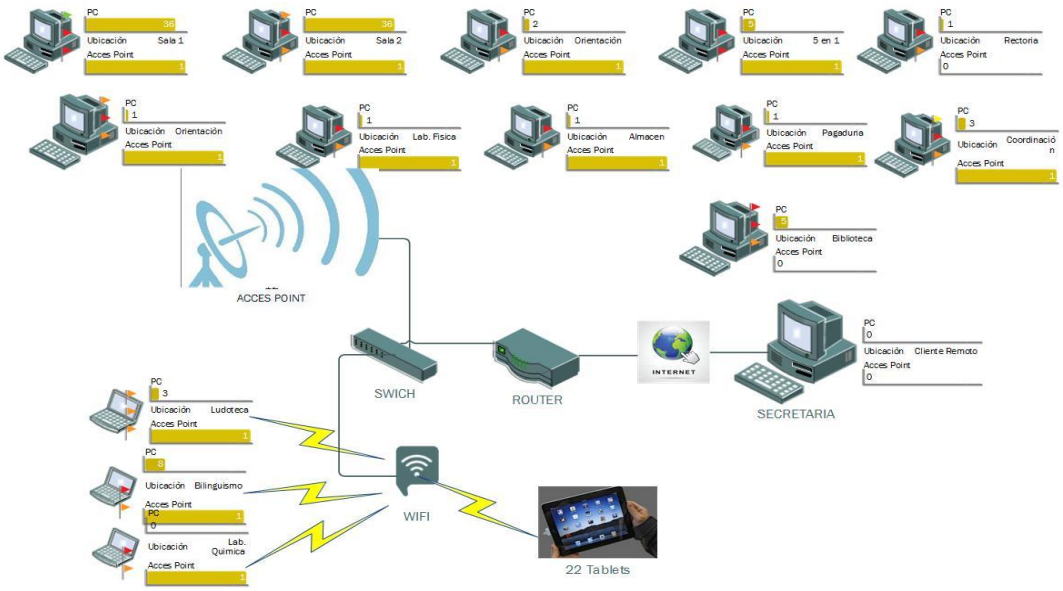
- ✓ TIC: Las TIC le permitirán al estudiante introducirse en los conceptos básicos, aproximándolo a la asignatura de modo que este pueda contextualizase con las nociones y ejemplos propios de las Tecnologías de la Información y las comunicaciones. Con este curso se espera que el estudiante se apropie de conceptos y fundamentos teóricos básicos sobre las TIC en donde se tendrá en cuenta los conceptos, su funcionalidad, los casos prácticos, usos y aplicaciones, conclusión y resumen. Las herramientas a utilizar: Correo electrónico, Internet, plataforma Moodle.

- ✓ Sistemas Operativos: tiene como finalidad orientar a los estudiantes en el reconocimiento de los sistemas operativos como un componente lógico que impacta el desarrollo tecnológico de la humanidad. Así mismo los sistemas operativos cobran un valor en el desarrollo tecnológico, ya que este elemento se encarga de automatizar el funcionamiento del hardware, aprovechando los recursos del sistema tecnológico. Los sistemas a utilizar son: Windows, Linux.

3.3.1.6 Infraestructura tecnológica

La infraestructura Tecnológica del Colegio Luis Carlos Galán Sarmiento está compuesta con ISP de ETB, el cual está conectado a un Router Cisco y éste a un Rack (Swicht) que reparte el servicio de Internet a todo el colegio; adicionalmente cuenta con 12 Acces point, 95 portátiles, 103 PC’S, 22 móviles (tablets), 97 portàtiles y 1 tablero wifi.

Figura 8. Infraestructura Tecnológica CLCGS



Fuente: Propiedad de los autores

3.3.1.7 Políticas de uso para la utilización de los PC

- ✓ Registrar en la bitácora el estado de los computadores.
- ✓ No introducir USB sin previa autorización.
- ✓ No rayar el computador.
- ✓ No instalar programas sin autorización.
- ✓ Utilizar los computadores de manera adecuada y eficiente.
- ✓ Todos los computadores deben ser apagados cuando termine la sección de clase.
- ✓ Cada estudiante debe responder por su equipo asignado.
- ✓ En caso de que un computador vaya a ser utilizado por otra persona diferente a la que asignó, este último debe asegurar y velar por el buen uso de dicho recurso.
- ✓ No cambiar la configuración del equipo de cómputo.
- ✓ La protección física de los computadores, corresponden a las personas asignadas, y es su deber notificar al docente encargado, sobre cualquier eventualidad encontrada o que pueda ocurrir durante su proceso de trabajo.
- ✓ La instalación de software, hardware, reparación o retiro de cualquier pieza del computador, solo puede ser realizado por funcionarios autorizados, Redp(red Integrada de Participación Educativa-Colombia).
- ✓ Solo se permite conectarse a la red del colegio aquellas personas autorizadas para ello.
- ✓ Se prohíbe la conexión de celulares en los zócalos asignados a las conexiones eléctricas de los computadores.

3.3.1.8 Políticas de uso para la utilización de INTERNET

- ✓ Dar buen uso a las redes sociales.
- ✓ Hago uso de mi identidad de manera segura en mi interacción con otros en los ambientes tecnológicos
- ✓ Utilizo las TIC para mi libre desarrollo de autoridad y autonomía, y a través de ella reconozco y hago respetar mis creencias y pensamientos, y los de los demás.
- ✓ No ingresar a páginas no permitidas.
- ✓ No se permitirá el uso redes sociales en ningún horario a menos que el Docente lo autorice.
- ✓ El estudiante no debe descargar ningún programa sin la debida autorización.
- ✓ El estudiante no debe abrir ni revisar correos electrónicos inseguros o con dudosa procedencia.
- ✓ Se prohíbe a los estudiantes cualquier transmisión vía Internet que no sea autorizada.
- ✓ No hacer hacking

3.4 SISTEMAS DE INFORMACIÓN

Los sistemas de información que cuenta el Colegio Luis Carlos Galán Sarmiento son Herramienta Chip, para el área contable, suministrado por la secretaria de educación; además, hay otros servicios que presta el área de sistemas por REDP para el apoyo informático académico:

- ✓ DFD. Software para elaboración de diagrama de flujo.
- ✓ Pseint: Herramienta algorítmica para la iniciación de programas.
- ✓ Cabri-Geom: Software matemático para la enseñanza de geometría plana.
- ✓ Crocodile: Software simulador de circuitos eléctricos.
- ✓ Deep-Freze 7: Es un congelador que se encuentra instalado en todos los computadores para evitar guardar archivos permanentes en el computador.
- ✓ Derive-Matem: Programa que se utiliza para realizar problemas matemáticos: Calculo – Algebra.
- ✓ Dev-C++ Portable: Lenguaje para programar en C++.
- ✓ Gimp: Programa gratuito para edición y manipulación de imagen.
- ✓ WinCmapTools: Software para la construcción de Mapas conceptuales.
- ✓ MicromundosPro: Lenguaje de programación Logo. Los estudiantes piensan y resuelven situaciones.
- ✓ Photoshop CS4 Portable_j89: Programa para el retoque fotográfico.
- ✓ TuxPaint: Software libre para dibujar.
- ✓ LEGO DIGITAL DESIGNER: Programa para construcción de LEGO.
- ✓ Macromedia_Flash_8_(Portable): Es un programa de creación de animaciones vectoriales que utiliza el docente de Informàtica.
- ✓ MECA NET: Curso de mecanografía para estudiantes.
- ✓ Microsoft Mathematics 4.0: Software para resolver problemas matemáticos y científicos.

Figura 9. Herramienta Chip

Fuente: Secretaria de Educación del Distrito. Presentación contable fondos de servicios educativos. [en línea]. [Citado el 03-12-17]. Disponible en: http://www.educacionbogota.edu.co/archivos/Temas%20estrategicos/FSE/2013/PRESENTACION_CONTABLE_FONDOS_DE_SERVICIOS_EDUCATIVOS.pdf

4. EVIDENCIAR LOS ACTIVOS DE LA INFORMACIÓN DE LA INSTITUCIÓN EDUCATIVA LUIS CARLOS GALÁN SARMIENTO MEDIANTE LA METODOLOGÍA DE MAGERIT

Para evidenciar los activos de la información, está monografía se basa en la metodología MAGERIT, activos que fueron evidenciados en el Colegio Luis Carlos Galán Sarmiento. Esta fase describe todo el contexto de la organización sobre el Conocimiento de la organización.

4.1 CLASIFICACIÓN DE LA INFORMACIÓN[63]

La Ley 1712 de 2014, artículo 18, en concordancia con la Ley 1266 de 2008 (Hábeas Data), indican que existe información que por su naturaleza no debe ser divulgada ya que puede atentar contra la intimidad de su propietario y solo es relevante para el titular. En ésta categoría se encuentra la información de carácter privado y semi-privado.

Para la clasificación de la información, se evalúan las tres características básicas como son: confidencialidad, integridad y disponibilidad.

Los criterios para asignar la calificación a las categorías de información son aquellos indicados por la Ley 1712 de 2014 que fue reglamentada con el Decreto 103 de 2015 y que además son reiterados en el Decreto reglamentario Único del Sector Presidencia de la República. De igual forma se aconseja apoyar éstos conceptos de calificación de la información de acuerdo a indicaciones proporcionadas por la Ley 594 de 2000 y decretos reglamentarios (Ley General de Archivos) y la Ley Estatutaria 1581 de 2012 y decretos reglamentarios (Sobre el tratamiento de los datos personales).

Tabla 4. Clasificación de la información

Criterio	Definición
Secreta	La información reservada es aquélla que, por motivos excepcionales, se declara como tal por parte del jerarca del organismo, a los efectos de impedir su acceso público. Es clave la formulación excepcional, la necesidad de justificar que es imperioso y necesario mantener una información reservada porque afecta un interés legítimo del Estado.

[63] SIGEPRE. Presidencia de la república. Guía para la calificación de la información de acuerdo con sus niveles de seguridad. [en línea] [citado el 04-12_2017]. Disponible en: http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/G-GD-02-calificacion-informacion.pdf

CRITERIO	DEFINICIÒN
Secreta	Sólo puede ser declarada como tal por resolución fundada del jerarca máximo del organismo cuando se verifique alguna de las causales que prevé de manera taxativa la Ley de Acceso a la Información pública[64].
Confidencial	Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma[65].
Reservada-uso interno	Es la información manejada por los directivos, docentes, estudiantes y demás miembros del colegio con derecho a privilegios con algunos derechos de manipulación de información.
Publica	Información que es de manejo público.

Fuente: SIGEPRE. Presidencia de la república. Guía para la calificación de la información de acuerdo con sus niveles de seguridad. [En línea] [Citado el 04-12_2017]. Disponible en: http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/G-GD-02-calificacion-informacion.pdf

4.2 ACTIVOS INFORMÁTICOS

En la tabla 5 se puede observar los activos más relevantes que se encuentra dentro de la institución Luis Carlos Galán Sarmiento, esta clasificación se hace en base a la metodología MAGERIT

[64] UAP. UNIVERSIDAD DE ACCESO A LA INFORMACIÒN PÚBLICA. Guía de la clasificación. [en línea] [citado el [10-12-2017]. Disponible en: http://www.uaip.gub.uy/wps/wcm/connect/uaip/f66e7798-91be-45f7-bae0-51c5e65a197e/Gu%C3%ADa_clasificaci%C3%B3n+VF+%281%29.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=f66e7798-91be-45f7-bae0-51c5e65a197e

[65] Corte constitucional república de Colombia. [citado el [10-12-2017]. Disponible en: http://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm

Tabla 5. Tipos de Activos

TIPO DE ACTIVO	CÓDIGO DE ACTIVO	ACTIVOS MÁS RELEVANTES EN LA ENTIDAD
[essencial] Activos Esenciales	[adm] Datos de interés para la administración pública	Contratos
		Acuerdos
	[vr] datos vitales	Registro de Calificaciones
	[per] datos de carácter personal	Base de datos de carácter personal.
		Contabilidad del colegio.
	[classified] Datos clasificados	Hoja de vida de los Estudiantes.
[D] datos / información	[Files] Ficheros:	Calificaciones
		Contabilidad
		Archivos de actas
		Resoluciones (Actos administrativos y académicos)
		Observador del alumno
		Libro de Matricula
	[backup] copias de respaldo	Contabilidad institucional
		Documentos administrativos
[S] Servicios	[edi] intercambio electrónico de datos	Diligenciamiento Matriz Chip
[SW] Software - Aplicaciones informáticas	[os] sistema operativo	Sistema operativo Windows 7, Windows 8
	[sub] Desarrollo a medida(Subcontratado)	Aplicación para el manejo de notas y reportes de los estudiantes.
	[dbms] sistema de gestión de bases de datos:	Base de datos para almacenar las notas de los estudiantes
	[office] ofimática:	Office 2013, winrar, Adobe Acrobat Reader.
	[av] antivirus	Microsoft Security Essentials.
	[std] estándar	Java, Cabri-Geom, Crocodile: Deep-Freze, Derive-Matem, Dev-C++ Portable, Gimp, WinCmapTools, MicromundosPro, Photoshop CS4 Portable_j89, TuxPaint, LEGO DIGITAL DESIGNER, Macromedia_Flash_8_(Portable), MECA NET, Microsoft Mathematics 4.0

TIPO DE ACTIVO	CÓDIGO DE ACTIVO	ACTIVOS MÁS RELEVANTES EN LA ENTIDAD
[HW] Equipamiento informático (hardware)	[pc] informática personal	72 Equipos de escritorio salas de sistemas
		12 equipos de escritorio aulas especializadas
		19 equipos de escritorio zona administrativa
	[mobile] informática móvil	95 Portátiles aulas especializadas
	[wap] punto de acceso inalámbrico	12 antenas de Access point
	[switch] conmutadores	4 switch 24 puertos
	[router] encaminadores	Router CISCO 2900 Series.
	[print] equipos de impresión:	2 Impresoras salas de sistemas
		2 impresoras de multifunción (zona administrativa) 1 impresora chorro de tinta (zona administrativa) 1 impresora inalámbrica (zona administrativa)
[COM] Redes de comunicaciones	[PSTN] red telefónica	Acceso telefónico ETB
	[LAN] red local	Red LAN
	[wifi] red inalámbrica	Red Inalámbrica
	[Internet] Internet	ETB
[Media] Soportes de información	[cd] cederrón (CD-ROM)	Actas, resoluciones, observador de los estudiantes, agendas telefónicas, fotografías de los estudiantes por cursos, Soporte de contabilidad.
	[usb] memorias USB	Copia de seguridad, documentos
	[dvd] DVD	Proyecto educativo institucional, actas institucionales, documentos institucionales.
		Copia de Seguridad notas
	[printed] material impreso	Actas, resoluciones, observador del estudiantes, agenda telefónicas, fotografías de los estudiantes por cursos, Soporte de contabilidad, boletines, informes académicos, constancias, etc.
[AUX] Equipamiento auxiliar	[wire] cable eléctrico	Instalaciones para el suministro de energía
	[furniture] mobiliario	rack, armarios, archivadores, mesas, muebles, etc
[L] Instalaciones	[building] edificio	Edificio sede colegio Luis Carlos Galán Sarmiento
[P] Personal	[ue] usuarios externos	REDP
	[ui] usuarios internos	Administrativos, docentes
	[adm] administradores de sistemas	Docente de media Integrada e Informática
	[prov] proveedores	REDP, ETB

Fuente: Propiedad de los autores

4.3 CLASIFICACIÓN DE LOS ACTIVOS DE LA INFORMACIÓN

Los activos de información deben ser clasificados de acuerdo a los criterios de información: Secreta, Confidencial, Reservada-Uso Interno y Publica; con el objetivo de clasificarlos, tratarlos y protegerlos, ver tabla 8.

Tabla 6. Clasificación de los activos

TIPO DE ACTIVO	CÓDIGO DE ACTIVO	ACTIVOS MÁS RELEVANTES EN LA ENTIDAD	CLASIFICACION DE LA INFORMACION
[essencial] Activos Esenciales	[adm] Datos de interés para la administración pública	Contratos	Pública
		Acuerdos	Pública
	[vr] datos vitales	Registro de Calificaciones	Confidencial
	[per] datos de carácter personal	Base de datos de carácter personal.	Confidencial
		Contabilidad del colegio.	Reservada-Uso Interno
	[classified] Datos clasificados	Hoja de vida de los Estudiantes.	Confidencial
[D] datos / información	[Files] Ficheros:	Calificaciones	Confidencial
		Contabilidad	Confidencial
		Archivos de actas	Pública
		Resoluciones (Actos administrativos y académicos)	Pública
		Observador del alumno	Confidencial
		Libro de Matricula	Confidencial
	[backup] copias de respaldo	Contabilidad institucional	Confidencial
		Documentos administrativos	Reservada-Uso Interno
[S] Servicios	[edi] intercambio electrónico de datos	Diligenciamiento Matriz Chip	Confidencial
[SW] Software - Aplicaciones informáticas	[os] sistema operativo	Sistema operativo Windows 7, Windows 8	Pública
	[sub] Desarrollo a medida(Subcontratado)	Aplicación para el manejo de notas y reportes de los estudiantes.	Confidencial
	[dbms] sistema de gestión de bases de datos:	Base de datos para almacenar las notas de los estudiantes	Confidencial
	[office] ofimática:	Office 2013, winrar, Adobe Acrobat Reader.	Reservada-Uso Interno
	[av] antivirus	Microsoft Security Essentials.	Reservada-Uso Interno

TIPO DE ACTIVO	CÓDIGO DE ACTIVO	ACTIVOS MÁS RELEVANTES EN LA ENTIDAD	CLASIFICACION DE LA INFORMACION
[SW] Software - Aplicaciones informáticas	[std] estándar	Java, Cabri-Geom, Crocodile: Deep-Freze, Derive-Matem, Dev-C++ Portable, Gimp, WinCmapTools, MicromundosPro, Photoshop CS4 Portable_j89, TuxPaint, LEGO DIGITAL DESIGNER, Macromedia_Flash_8_(Portable), MECA NET, Microsoft Mathematics 4.0	Reservada-Uso Interno
[HW] Equipamiento informático (hardware)	[pc] informática personal	72 Equipos de escritorio salas de sistemas	Reservada-Uso Interno
		12 equipos de escritorio aulas especializadas	Reservada-Uso Interno
		19 equipos de escritorio zona administrativa	Reservada-Uso Interno
	[mobile] informática móvil	95 Portátiles aulas especializadas	Reservada-Uso Interno
	[wap] punto de acceso inalámbrico	12 antenas de Access Point	Reservada-Uso Interno
	[switch] conmutadores	4 switch 24 puertos	Reservada-Uso Interno
	[router] encaminadores	Router CISCO 2900 Series.	Reservada-Uso Interno
	[print] equipos de impresión:	2 Impresoras salas de sistemas	Reservada-Uso Interno
		2 impresoras de multifunción (zona administrativa) 1 impresora chorro de tinta (zona administrativa) 1 impresora inalámbrica (zona administrativa)	Reservada-Uso Interno
[COM] Redes de comunicaciones	[PSTN] red telefónica	Acceso telefónico ETB	Reservada-Uso Interno
	[LAN] red local	Red LAN	Reservada-Uso Interno
	[wifi] red inalámbrica	Red Inalámbrica	Reservada-Uso Interno
	[Internet] Internet	ETB	Reservada-Uso Interno

TIPO DE ACTIVO	CÓDIGO DE ACTIVO	ACTIVOS MÁS RELEVANTES EN LA ENTIDAD	CLASIFICACION DE LA INFORMACION
[Media] Soportes de información	[cd] cederrón (CD-ROM)	Actas, resoluciones, observador de los estudiantes, agendas telefónicas, fotografías de los estudiantes por cursos, Soporte de contabilidad.	Confidencial
	[usb] memorias USB	Copia de seguridad, documentos	Confidencial
	[dvd] DVD	Proyecto educativo institucional, actas institucionales, documentos institucionales.	Confidencial
		Copia de Seguridad notas	Confidencial
	[printed] material impreso	Actas, resoluciones, observador del estudiantes, agenda telefónicas, fotografías de los estudiantes por cursos, Soporte de contabilidad, boletines, informes académicos, constancias, etc.	Confidencial
[AUX] Equipamiento auxiliar	[wire] cable eléctrico	Instalaciones para el suministro de energía	Reservada-Uso Interno
	[furniture] mobiliario	rack, armarios, archivadores, mesas, muebles, etc	Reservada-Uso Interno
[L] Instalaciones	[building] edificio	Edificio sede colegio Luis Carlos Galán Sarmiento	Reservada-Uso Interno
[P] Personal	[ue] usuarios externos	REDP	Pública
	[ui] usuarios internos	Administrativos, docentes	Reservada-Uso Interno
	[adm] administradores de sistemas	Docente de media Integrada e Informática	Reservada-Uso Interno
	[prov] proveedores	REDP, ETB	Pública

Fuente: Propiedad de los autores

4.4 DIMENSIONES DE VALORACIÓN

Las dimensiones de valoración de los activos es el nivel de importancia que tiene éste en la entidad.

Teniendo en cuenta la valoración cualitativa del impacto y a la seguridad del mismo se evalúa los activos del colegio Luis Carlos Galán Sarmiento.

4.4.1 DE ACUERDO AL IMPACTO

Se realiza una evaluación cualitativa según el impacto que èste pueda tener, teniendo en cuenta el tamaño del daño que puede ocasionar al colegio Luis Carlos Galán Sarmiento.

4.4.1.1 Criterios de valoración

La escala de valoración está entre 0 (sin daños) hasta 10 (Valor máximo de daño en el activo), y se determina de acuerdo al tipo cualitativo y el impacto que tiene la institución educativa ver tabla 7.

Tabla 7. Criterio de Valoración.

IMPACTO	NOMENCLATURA	VALOR	DESCRIPCIÓN
MUY ALTO	MA	10	El daño tiene consecuencias muy graves para la institución educativa y podrían ser irreversibles.
ALTO	A	7 - 9	El daño tiene consecuencias muy graves para la institución educativa.
MEDIO	M	4 - 6	El daño contiene consecuencias relevantes para la institución educativa y su operación.
BAJO	B	1 - 3	El daño contiene consecuencias relevantes, pero no afecta a una gran parte de la institución educativa.
MUY BAJO	MB	0	El daño no contiene consecuencias relevantes para la institución educativa.

Fuente: Propiedad de los autores

4.4.1.2 Valoración de los activos

Las tablas siguientes pretenden guiar con más detalle a los usuarios valorando de forma homogénea activos cuyo valor es importante por diferentes motivos.

Tabla 8. Escala Estándar Información de carácter personal

[pi] Información de carácter personal		
6	6.pi1	probablemente afecte gravemente a un grupo de individuos
	6.pi2	probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
5	5.pi1	probablemente afecte gravemente a un individuo
	5.pi2	probablemente quebrante seriamente leyes o regulaciones
4	4.pi1	probablemente afecte a un grupo de individuos
	4.pi2	probablemente quebrante leyes o regulaciones

[pi] Información de carácter personal		
3	3.pi1	probablemente afecte a un individuo
	3.pi2	probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	pudiera causar molestias a un individuo
	2.pi2	pudiera quebrantar de forma leve leyes o regulaciones
1	1.pi1	pudiera causar molestias a un individuo

Fuente: GOBIERNO DE ESPAÑA. Magerit - versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro II - Catálogo de elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012. P. 19.

Tabla 9. Escala Estándar Obligaciones legales

[lpo] Obligaciones legales		
9	9.lro	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lro	probablemente cause un incumplimiento grave de una ley o regulación
5	5.lro	probablemente sea causa de incumplimiento de una ley o regulación
1	1.lro	pudiera causar el incumplimiento leve o técnico de una ley o regulación

Fuente: ibid. p 20.

Tabla 10. Escala Estándar Seguridad

[si] Seguridad		
10	10.si	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
9	9.si	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
7	7.si	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3	3.si	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1	1.si	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

Fuente: ibid. p 20.
.

Tabla 11. Escala Estándar Intereses comerciales o económicos

[cei] Intereses comerciales o económicos		
9	9.cei.a	de enorme interés para la competencia
	9.cei.b	de muy elevado valor comercial
	9.cei.c	causa de pérdidas económicas excepcionalmente elevadas
	9.cei.d	Causa de muy significativas ganancias o ventajas para individuos u organizaciones.
	9.cei.e	constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7	7.cei.a	de alto interés para la competencia
	7.cei.b	de elevado valor comercial
	7.cei.c	causa de graves pérdidas económicas
	7.cei.d	proporciona ganancias o ventajas desmedidas a individuos u organizaciones
	7.cei.e	constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
3	3.cei.a	de cierto interés para la competencia
	3.cei.b	de cierto valor comercial
	3.cei.c	causa de pérdidas financieras o merma de ingresos
	3.cei.d	facilita ventajas desproporcionadas a individuos u organizaciones
	3.cei.e	constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
2	2.cei.a	de bajo interés para la competencia
	2.cei.b	de bajo valor comercial
1	1.cei.a	de pequeño interés para la competencia
	1.cei.b	de pequeño valor comercial
0	0.3	supondría pérdidas económicas mínimas

Fuente: ibid. p 20 - 21

Tabla 12. Escala Estándar Interrupción del servicio

[da] Interrupción del servicio		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones.
	9.da2	Probablemente tenga un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la interrupción de actividades propias de la Organización

Fuente: ibid. p 21.

Tabla 13. Escala Estándar Orden Público

[po] Orden público		
9	9.po	alteración sería del orden público
6	6.po	probablemente cause manifestaciones, o presiones significativas
3	3.po	causa de protestas puntuales
1	1.po	pudiera causar protestas puntuales

Fuente: ibid. p 21.

Tabla 14. Escala Estándar Operaciones

[olm] Operaciones		
10	10.olm	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	9.olm	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7	7.olm	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

[olm] Operaciones		
5	5.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3	3.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1	1.olm	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)

Fuente: ibid. p 21.

Tabla 15. Escala Estándar Administración y Gestión

[adm] Administración y gestión		
9	9.adm	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7	7.adm	probablemente impediría la operación efectiva de la Organización
5	5.adm	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3	3.adm	Probablemente impediría la operación efectiva de una parte de la Organización.
1	1.adm	Pudiera impedir la operación efectiva de una parte de la Organización.

Fuente: ibid. p 22.

Tabla 16. Escala Estándar Pérdida de confianza (reputación)

[lg] Pérdida de confianza (reputación)		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones.
	5.lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público

[lg] Pérdida de confianza (reputación)		
3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.4	no supondría daño a la reputación o buena imagen de las personas u organizaciones

Fuente: ibid. p 22.

Tabla 17. Escala Estándar Persecución de delitos

[crm] Persecución de delitos		
8	8.crm	Impida la investigación de delitos graves o facilite su comisión
4	4.crm	Dificulte la investigación o facilite la comisión de delitos

Fuente: ibid. p 22.

Tabla 18. Escala Estándar tiempo de recuperación del servicio

[rto] Tiempo de recuperación del servicio		
7	7.rto	RTO < 4 horas
4	4.rto	4 horas < RTO < 1 día
1	1.rto	1 día < RTO < 5 días
0	0.rto	5 días < RTO

Fuente: ibid. p 22 - 23.

Tabla 19. Escala Estándar Información Clasificada (Nacional)

[lbl.nat] Información clasificada (nacional)		
10	10.lbl	Secreto
9	9.lbl	Reservado
8	8.lbl	Confidencial
7	7.lbl	Confidencial
6	6.lbl	Difusión limitada
5	5.lbl	Difusión limitada

Fuente: ibid. p 23.

[lbl.nat] Información clasificada (nacional)		
4	4.lbl	Difusión limitada
3	3.lbl	Difusión limitada
2	2.lbl	Sin clasificar
1	1.lbl	Sin clasificar

En la Tabla 20 se encuentra la valoración del impacto de los activos de la información del colegio Luis Carlos Galán Sarmiento.

Tabla 20. Valoración Activos

TIPO DE ACTIVO	CÓDIGO DE ACTIVO	DESCRIPCIÓN	IMPACTO	RAZON
[essencial] Activos Esenciales	[adm]	Contratos	M	Son esenciales para la adquisición de bienes y servicios para la institución.
		Acuerdos	M	Son documentos esenciales para las relaciones con otros estamentos o entes gubernamentales.
	[vr]	Registro de Calificaciones	A	Datos esenciales que permite visualizar el desempeño académico de los estudiantes.
	[per]	Base de datos de carácter personal.	A	Permiten guardar información personal de administrativos, docentes y estudiantes
		Contabilidad del colegio	MA	Proceso esencial que permite visualizar la economía de la institución, la cual es requerida por entes de control del estado.
	[classified]	Hoja de vida de los Estudiantes.	A	Información propia del estudiante, donde se almacena datos personales.

TIPO DE ACTIVO	CÓDIGO DE ACTIVO	DESCRIPCIÓN	IMPACTO	RAZON
[D] datos / información	[Files]	Calificaciones	A	Son documentos donde se almacenan las notas del seguimiento periódico del estudiante.
		Contabilidad	MA	Documentos donde se puede visualizar los estados financieros de la institución educativa.
		Archivos de actas	M	Información donde se consigna los datos de las diferentes reuniones que se llevan a cabo en la institución
		Resoluciones (Actos administrativos y académicos)	M	Documentos donde se emiten diferentes actos de índole administrativo o académico.
		Observador del alumno	M	Documento donde se encuentra consignado el seguimiento del estudiante durante un período académico en la parte comportamental.
		Libro de Matricula	MA	Libro donde se encuentra matriculados los estudiantes de la institución.
	[backup]	Contabilidad institucional	A	Copia de seguridad de los archivos Excel, Word, que se generan en el área de contabilidad.
		Documentos administrativos	A	Copia de seguridad de los actos administrativos, registro de notas, seguimientos académicos.
[S] Servicios	[edi]	Diligenciamiento Matriz Chip	MA	Registro del seguimiento a la contabilidad solicitada por la secretaría de educación de Bogotá D.C.

TIPO DE ACTIVO	CÓDIGO DE ACTIVO	DESCRIPCIÓN	IMPACTO	RAZON
[SW] Software - Aplicaciones informáticas	[os]	Sistema operativo Windows 7, Windows 8	M	Administra los recursos hardware y software de los diferentes computadores que tiene la institución
	[sub]	Aplicación para el manejo de notas y reportes de los estudiantes.	M	Utilizado para el registro de notas de los estudiantes para el seguimiento académico.
	[dbms]	Base de datos para almacenar las notas de los estudiantes	A	Utilizado para el almacenamiento final de las notas académicas de los estudiantes.
	[office]	Office 2013, winrar, Adobe Acrobat Reader.	B	Utilizado para tareas básicas dentro de la institución por la parte administrativa y académica.
	[av]	Microsoft Security Essentials.	M	Utilizado para prevenir software malicioso en los equipos de cómputo de la institución.
	[std]	Java, Cabri-Geom, Crocodile: Deep-Freze, Derive-Matem, Dev-C++ Portable, Gimp, WinCmapTools, MicromundosPro, Photoshop CS4 Portable_j89, TuxPaint, LEGO DIGITAL DESIGNER, Macromedia_Flash_8_(Portable), MECA NET, Microsoft Mathematics 4.0	M	Aplicativos suministrados por REDP para el desarrollo de actividades académicas en las asignaturas de Tecnología e Informática.

TIPO DE ACTIVO	CÓDIGO DE ACTIVO	DESCRIPCIÓN	IMPACTO	RAZON
[HW] Equipamiento informático (hardware)	[pc]	72 Equipos de escritorio salas de sistemas	B	Dispositivos para la ejecución de tareas en la parte administrativa y académica.
		12 equipos de escritorio aulas especializadas	B	Dispositivos para la ejecución de tareas en la parte administrativa y académica.
		19 equipos de escritorio zona administrativa	B	Dispositivos para la ejecución de tareas en la parte administrativa y académica.
	[mobile]	95 Portátiles aulas especializadas	B	Dispositivos para la ejecución de tareas en la parte administrativa y académica.
	[wap]	12 antenas de Access Point	M	Dispositivo esencial para establecer comunicación en toda el área que comprende la institución
	[switch]	4 switch 24 puertos	M	Dispositivo esencial para direccionar los datos a través de la red LAN.
	[router]	Router CISCO 2900 Series.	M	Dispositivo esencial para establecer el enlace entre el colegio y el ISP.
	[print]	2 Impresoras salas de sistemas	B	Dispositivo para realizar impresiones sobre papel, por la parte administrativa y académica.
		2 impresoras de multifunción (zona administrativa) 1 impresora chorro de tinta (zona administrativa) 1 impresora inalámbrica (zona administrativa)	B	Dispositivo para realizar impresiones sobre papel, por la parte administrativa y académica.
[COM] Redes de comunicaciones	[PSTN]	Acceso telefónico ETB	B	Servicio para establecer comunicación desde la institución a diferentes entes públicos y privados.
	[LAN]	Red LAN	MA	Esencial para la trasmisión de datos y proveer los diferentes servicios que utiliza la institución para su normal funcionamiento.
	[wifi]	Red Inalámbrica	MA	Dispositivos esenciales para ampliar la cobertura que se tiene dentro de la institución educativa.
	[Internet]	ETB	M	Servicio que es suministrado por un ente externo.

TIPO DE ACTIVO	CÓDIGO DE ACTIVO	DESCRIPCIÓN	IMPACTO	RAZON
[Media] Soportes de información	[cd]	Actas, resoluciones, observador de los estudiantes, agendas telefónicas, fotografías de los estudiantes por cursos, Soporte de contabilidad.	A	Copias de respaldo de actas académicas, resoluciones, observador de los estudiantes, agenda telefónicas, fotografías de los estudiantes por cursos, Soporte de contabilidad
	[usb]	Copia de seguridad, documentos	A	Copias de respaldo de actas, resoluciones, observador de los estudiantes, agenda telefónicas, fotografías de los estudiantes por cursos, Soporte de contabilidad
	[dvd]	Proyecto educativo institucional, actas institucionales, documentos institucionales.	A	Copia de respaldo del PEI, actas institucionales y otros documentos administrativos.
		Copia de Seguridad notas	A	Copia de respaldo de notas académicas de estudiantes.
	[printed]	Actas, resoluciones, observador del estudiantes, agenda telefónicas, fotografías de los estudiantes por cursos, Soporte de contabilidad, boletines, informes académicos, constancias, etc.	A	Copia impresa debidamente almacenada en cajas de acuerdo a registro documental de: actas, resoluciones, observador del estudiantes, agenda telefónicas, fotografías de los estudiantes por cursos, Soporte de contabilidad, boletines, informes académicos, constancias, etc.
[AUX] Equipamiento auxiliar	[wire]	Instalaciones para el suministro de energía	M	Sistema esencial para el suministro de energía, el cual es suministrado por CODENSA.
	[furniture]	rack, armarios, archivadores, mesas, muebles, etc	B	Esencial para el funcionamiento de la parte administrativa y académica, almacenamiento de archivo físico, y organización de los dispositivos intermedios de comunicaciones.
[L] Instalaciones	[building]	Edificio sede colegio Luis Carlos Galán Sarmiento	MA	Esencial para el funcionamiento de la institución educativa Luis Carlos Galán Sarmiento

TIPO DE ACTIVO	CÓDIGO DE ACTIVO	DESCRIPCIÓN	IMPACTO	RAZON
[P] Personal	[ue]	REDP	A	La secretaria de Educación hace acompañamiento técnico en mantenimiento a través de la Red Integrada de Participación Educativa (REDP) , que hace parte de un proyecto Transformador Pedagógico de la Escuela y la enseñanza; donde ésta maneja todo el sistema informático
	[ui]	Administrativos, docentes	MA	Personal que componen la comunidad educativa de la institución Luis Carlos Galán Sarmiento.
	[adm]	Docente de media Integrada e Informática	A	Personal de área de sistemas
	[prov]	REDP, ETB	M	Servicios suministrados por entes externos

Fuente: Propiedad de los autores

4.4.2 DE ACUERDO A LAS DIMENSIONES DE SEGURIDAD

Las dimensiones de seguridad están dados por aquellos atributos esenciales en la seguridad de la información que hacen valido un activo; ellos son: disponibilidad [D], confidencialidad de la información [C], integridad de datos [I], Autenticidad [A] y trazabilidad [T].

4.4.2.1 Criterios de valoración

La escala de valoración de la Tabla 9 se utiliza para valorar los activos de la información de acuerdo a las dimensiones de seguridad, esta escala nos permite valorar de manera cualitativa los activos del Colegio Luis Carlos Galán Sarmiento.

4.4.2.2 Valoración de activos

En la tabla 23 se encuentra la valoración de los activos de la institución Luis Carlos Galán Sarmiento de acuerdo a las dimensiones de seguridad, para lo cual se tendrá en cuenta las tablas 10 a la 21, lo que nos permitirá una valoración de manera cualitativa.

[INFO] INFORMACIÓN

En la tabla 21 se puede observar las valoraciones de los activos [Info] información del Colegio Luis Carlos Galán Sarmiento de acuerdo a las dimensiones de seguridad.

Tabla 21. Dimensiones de seguridad - [INFO] INFORMACIÓN

CÓDIGO DE ACTIVO	DESCRIPCIÓN	DIMENSIONES DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
[adm]	Contratos		5			
	Acuerdos		5			
[vr]	Registro de Calificaciones		6	7	6	6
[per]	Base de datos de carácter personal.		6	7	6	6
	Contabilidad del colegio	9	9	9	9	
[classified]	Hoja de vida de los Estudiantes.		6	7	6	6

CÓDIGO DE ACTIVO	DIMENSIONES DE SEGURIDAD	DESCRIPCION
[adm]	[I]	5.adm probablemente impediría la operación efectiva de más de una parte de la Organización
[vr]	[I][A][T]	6.pi1 probablemente afecte gravemente a un grupo de individuos
	[C]	7.lro: Probablemente cause un incumplimiento grave de una ley o regulación
[per]	[I][A][T]	6.pi2 probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
	[C]	7.lro: Probablemente cause un incumplimiento grave de una ley o regulación
	[D][I][C][A]	9.lro probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
[classified]	[I][A][T]	6.pi1 probablemente afecte gravemente a un grupo de individuos
	[C]	7.lro: Probablemente cause un incumplimiento grave de una ley o regulación

Fuente: Propiedad de los autores

[D] DATOS / INFORMACIÓN

En la tabla 22 se puede observar las valoraciones de los activos [D] Datos / Información del Colegio Luis Carlos Galán Sarmiento de acuerdo a las dimensiones de seguridad.

Tabla 22. Dimensiones de seguridad - [D] DATOS / INFORMACIÓN

CÓDIGO DE ACTIVO	DESCRIPCIÓN	DIMENSIONES DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
[Files]	Calificaciones		6	7	6	6
	Contabilidad	**9**	9	9	9	
	Archivos de actas		3			3
	Resoluciones (Actos administrativos y académicos)		5	5		6
	Observador del alumno		6	5		
	Libro de Matricula	**9**	9			
[backup]	Contabilidad institucional	**3**		2		
	Documentos administrativos	**3**		2		

CÓDIGO DE ACTIVO	DIMENSIONES DE SEGURIDAD	DESCRIPCION
[Files]	[I][A][T]	6.pi1 probablemente afecte gravemente a un grupo de individuos
	[C]	7.lro: Probablemente cause un incumplimiento grave de una ley o regulación
	[I][C]	5.lro probablemente sea causa de incumplimiento de una ley o regulación
	[D][I][C][A]	9.lro probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
	[I][T]	3.lro probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
[backup]	[D]	3. adm: Probablemente impediría la operación efectiva de una parte de la Organización.
	[C]	2. lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización.

Fuente: Propiedad de los autores

[S] SERVICIOS

En la tabla 25 se puede observar las valoraciones de los activos [S] Servicios del Colegio Luis Carlos Galán Sarmiento de acuerdo a las dimensiones de seguridad.

Tabla 23. Dimensiones de seguridad - [S] SERVICIOS

CÓDIGO DE ACTIVO	DESCRIPCIÓN	DIMENSIONES DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
[edi]	Diligenciamiento Matriz Chip	9	9	9		

CÓDIGO DE ACTIVO	DIMENSIONES DE SEGURIDAD	DESCRIPCION
[edi]	[D][I][C]	9.da Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones

Fuente: Propiedad de los autores

[SW] SOFTWARE - APLICACIONES INFORMÁTICAS

A continuación se puede observar las valoraciones de los activos [SW] SOFTWARE - APLICACIONES INFORMÁTICAS del Colegio Luis Carlos Galán Sarmiento de acuerdo a las dimensiones de seguridad, ver tabla 24

Tabla 24. Dimensiones de seguridad - [SW] SOFTWARE - APLICACIONES INFORMÁTICAS

CÓDIGO DE ACTIVO	DESCRIPCIÓN	DIMENSIONES DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
[os]	Sistema operativo Windows 7, Windows 8	5	7			
[sub]	Aplicación para el manejo de notas y reportes de los estudiantes.	7	7	7	7	
[dbms]	Base de datos para almacenar las notas de los estudiantes	7	7	7	7	
[office]	Office 2013, winrar, Adobe Acrobat Reader.	1				
[av]	Microsoft Security Essentials.	5		7		
[std]	Java, Cabri-Geom, Crocodile: Deep-Freze, Derive-Matem, Dev-C++ Portable, Gimp, WinCmapTools, MicromundosPro, Photoshop CS4 Portable_j89, TuxPaint, LEGO DIGITAL DESIGNER, Macromedia_Flash_8_(Portable), MECA NET, Microsoft Mathematics 4.0	5				

CÓDIGO DE ACTIVO	DIMENSIONES DE SEGURIDAD	DESCRIPCION
[os]	[D]	5.adm probablemente impediría la operación efectiva de más de una parte de la Organización
	[I]	7.adm probablemente impediría la operación efectiva de la Organización
[sub]	[D][I][C][A]	7.adm probablemente impediría la operación efectiva de la Organización

CÓDIGO DE ACTIVO	DIMENSIONES DE SEGURIDAD	DESCRIPCION
[dbms]	[D][I][C][A]	7.adm probablemente impediría la operación efectiva de la Organización
[office]	[D]	1.da Pudiera causar la interrupción de actividades propias de la Organización
[av]	[D]	5.da Probablemente cause la interrupción de actividades propias de la Organización
	[C]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
[std]	[D]	5.da Probablemente cause la interrupción de actividades propias de la Organización

Fuente: Propiedad de los autores

[HW] EQUIPAMIENTO INFORMÁTICO (HARDWARE)

En la tabla 25 se puede observar las valoraciones de los activos [HW] EQUIPAMIENTO INFORMÁTICO (HARDWARE) del Colegio Luis Carlos Galán Sarmiento de acuerdo a las dimensiones de seguridad.

Tabla 25. . Dimensiones de seguridad - [HW] EQUIPAMIENTO INFORMÁTICO (HARDWARE)

CÓDIGO DE ACTIVO	DESCRIPCIÓN	DIMENSIONES DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
[pc]	72 Equipos de escritorio salas de sistemas	1				
	12 esquipos de escritorio aulas especializadas	1				
	19 equipos de escritorio zona administrativa	1				
[mobile]	95 Portaltiles aulas especializadas	1				
[wap]	12 antenas de access point	1				
[switch]	4 switch 24 puertos	5			7	
[router]	Router CISCO 2900 Series.	5			7	
[print]	2 Impresoras salas de sistemas	1				
	2 impresoras de multifunción (zona administrativa) 1 impresora chorro de tinta (zona administrativa) 1 impresora inalambrica (zona administrativa)	1				

CÓDIGO DE ACTIVO	DIMENSIONES DE SEGURIDAD	DESCRIPCION
[pc]	[D]	1.da Pudiera causar la interrupción de actividades propias de la Organización
[mobile]	[D]	1.da Pudiera causar la interrupción de actividades propias de la Organización
[wap]	[D]	1.da Pudiera causar la interrupción de actividades propias de la Organización
[switch]	[D]	5.da Probablemente cause la interrupción de actividades propias de la Organización
	[A]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
[router]	[D]	5.da Probablemente cause la interrupción de actividades propias de la Organización
	[A]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
[print]	[D]	1.da Pudiera causar la interrupción de actividades propias de la Organización
CÓDIGO DE ACTIVO	DIMENSIONES DE SEGURIDAD	DESCRIPCION
[PSTN]	[D]	1.adm pudiera impedir la operación efectiva de una parte de la Organización
[LAN]	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
[wifi]	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
[Internet]	[D]	3.da Probablemente cause la interrupción de actividades propias de la Organización

Fuente: Propiedad de los autores

[COM] REDES DE COMUNICACIONES

En la tabla 26 se puede observar las valoraciones de los activos [COM] REDES DE COMUNICACIONES del Colegio Luis Carlos Galán Sarmiento de acuerdo a las dimensiones de seguridad.

Tabla 26. Dimensiones de seguridad - [COM] REDES DE COMUNICACIONES

CÓDIGO DE ACTIVO	DESCRIPCIÓN	DIMENSIONES DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
[PSTN]	Acceso telefónico ETB	1				
[LAN]	Red Lan	5				
[wifi]	Red Inalámbrica	5				
[Internet]	ETB	3				

CÓDIGO DE ACTIVO	DIMENSIONES DE SEGURIDAD	DESCRIPCION
[PSTN]	[D]	1.adm pudiera impedir la operación efectiva de una parte de la Organización
[LAN]	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
[wifi]	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
[Internet]	[D]	3.da Probablemente cause la interrupción de actividades propias de la Organización

Fuente: Propiedad de los autores

[MEDIA] SOPORTES DE INFORMACIÓN

En la tabla 27 se puede observar las valoraciones de los activos [MEDIA] SOPORTES DE INFORMACIÓN del Colegio Luis Carlos Galán Sarmiento de acuerdo a las dimensiones de seguridad.

Tabla 27. Dimensiones de seguridad - [MEDIA] SOPORTES DE INFORMACIÓN

CÓDIGO DE ACTIVO	DESCRIPCIÓN	DIMENSIONES DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
[cd]	Actas, resoluciones, observador de los estudiantes, agendas telefónicas, fotografías de los estudiantes por cursos, Soporte de contabilidad.	3	6	2		
[usb]	Copia de seguridad, documentos	3	6	2		
[dvd]	Proyecto educativo institucional, actas institucionales, documentos institucionales.	3	6	2		
	Copia de Seguridad notas	5	6			6
[printed]	Actas, resoluciones, observador del estudiantes, agenda telefónicas, fotografías de los estudiantes por cursos, Soporte de contabilidad, boletines, informes académicos, constancias, etc.	3		3		6

CÓDIGO DE ACTIVO	DIMENSIONES DE SEGURIDAD	DESCRIPCION
[cd]	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
	[I]	6.pi2: Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
[usb]	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
	[I]	6.pi2: Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
[dvd]	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
	[I]	6.pi2: Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[I]	6.pi2: Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
[printed]	[D][C]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
	[T]	6.pi2: Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal

Fuente: Propiedad de los autores

[AUX] EQUIPAMIENTO AUXILIAR

En la tabla 28 se puede observar las valoraciones de los activos [AUX] EQUIPAMIENTO AUXILIAR del Colegio Luis Carlos Galán Sarmiento de acuerdo a las dimensiones de seguridad.

Tabla 28. Dimensiones de seguridad - [AUX] EQUIPAMIENTO AUXILIAR

CÓDIGO DE ACTIVO	DESCRIPCIÓN	DIMENSIONES DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
[wire]	Instalaciones para el suministro de energía	3				
[furniture]	rack, armarios, archivadores, mesas, muebles, etc	1				

CÓDIGO DE ACTIVO	DIMENSIONES DE SEGURIDAD	DESCRIPCION
[wire]	[D]	3.da Probablemente cause la interrupción de actividades propias de la Organización
[furniture]	[D]	1.da Pudiera causar la interrupción de actividades propias de la Organización

Fuente: Propiedad de los autores

[L] INSTALACIONES

En la tabla 29 se puede observar las valoraciones de los activos [L] INSTALACIONES del Colegio Luis Carlos Galán Sarmiento de acuerdo a las dimensiones de seguridad.

Tabla 29. Dimensiones de seguridad - [AUX] EQUIPAMIENTO AUXILIAR

CÓDIGO DE ACTIVO	DESCRIPCIÓN	DIMENSIONES DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
[building]	Edificio sede colegio Luis Carlos Galán Sarmiento	9				

CÓDIGO DE ACTIVO	DIMENSIONES DE SEGURIDAD	DESCRIPCION
[building]	[D]	9.da Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones

Fuente: Propiedad de los autores

[P] PERSONAL

En la tabla 32 se puede observar las valoraciones de los activos [P] PERSONAL del Colegio Luis Carlos Galán Sarmiento de acuerdo a las dimensiones de seguridad.

Tabla 30. Dimensiones de seguridad - [P] PERSONAL

CÓDIGO DE ACTIVO	DESCRIPCIÓN	DIMENSIONES DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
[ue]	REDP	7				
[ui]	Administrativos, docentes	9				
[adm]	Docente de media Integrada e Informática	7				
[prov]	REDP, ETB	3				
[prov]	[D]	3.adm probablemente impediría la operación efectiva de una parte de la Organización				

CÓDIGO DE ACTIVO	DIMENSIONES DE SEGURIDAD	DESCRIPCION
[ue]	[D]	7.olm Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[ui]	[D]	9.da Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
[adm]	[D]	7.adm probablemente impediría la operación efectiva de la Organización
[prov]	[D]	3.adm probablemente impediría la operación efectiva de una parte de la Organización

Fuente: Propiedad de los autores

5. AMENAZAS Y VULNERABILIDADES A LOS ACTIVOS DE LA INFORMACIÓN DE LA INSTITUCIÓN EDUCATIVA LUIS CARLOS GALÁN SARMIENTO MEDIANTE LA METODOLOGÍA DE MAGERIT

En la identificación de las amenazas y vulnerabilidades, se sigue lo planteado en la metodología MAGERIT V3 libro 2, se hace necesario realizar este análisis para determinar las amenazas y vulnerabilidades que pueden afectar los activos con que actualmente cuenta el Colegio Luis Carlos Galán Sarmiento.

5.1 IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS

A continuación se hace una descripción de las amenazas que se tendrán en cuenta de acuerdo a lo propuesto en la metodología MAGERIT Libro I:

5.1.1 De origen natural ([N] Desastres naturales)

Hay accidentes naturales (terremotos, inundaciones, etc). Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder[66].

5.1.2 Del entorno ([I] De origen industrial)

Hay desastres industriales (contaminación, fallos eléctricos, etc) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos[67].

5.1.3 Causadas por las personas de forma accidental ([E] Errores y fallos no intencionados)

Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión[68].

5.1.4 Causadas por las personas de forma deliberada ([A] Ataques intencionados)

Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse

[66] MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método, p. 27.
[67] Ibid. p.27.
[68] Ibid. p.27.

indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios[69].

En la Tabla 32 se hace un resumen de las amenazas de acuerdo a la metodología de MAGERIT V3, que se tienen en cuenta para el análisis.

Tabla 31. Valoración de amenazas

Nomenclatura	Tipos de amenazas
[N]	Desastres naturales
[I]	De origen industrial
[E]	Errores y fallos no intencionados
[A]	Ataques intencionados

Fuente: Propiedad de los autores

5.1.5 **Criterios de Evaluación**

Los criterios de valoración se muestran en una escala cualitativa y cuantitativa para la estimación del Riesgo que puede tener una entidad.

Tabla 32. Criterio Evaluación. Amenazas

PROBABILIDAD O FRECUENCIA	NOMENCLATURA	RANGO	VALOR
FRECUENCIA MUY ALTA	MA: INSEGURO	1 vez al día	100%
FRECUENCIA ALTO	A: PROBABLE	1 vez cada semana	75%
FRECUENCIA MEDIA	M: POSIBLE	1 vez cada 2 meses	50%
FRECUENCIA BAJA	B: POCO PROBABLE	1 vez cada 6 meses	25%
FRECUENCIA MUY BAJA	MB: MUY RARO	1 vez al año	10%

Fuente: Propiedad de los autores

5.1.6 Evaluación de las amenazas a los activos

En la valoración de las amenazas a los activos hallados en la investigación se valora la amenaza con su frecuencia.

5.1.6.1 [INFO] INFORMACIÓN

A continuación se hace la evaluación de las amenazas y el impacto que estas tienen sobre el activo [INFO] INFORMACIÓN, ver tabla 34.

[69] Ibid. p.27.

Tabla 33. Evaluación de amenazas - [INFO] INFORMACIÓN

ACTIVO	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Contratos	[E.1] Errores de los usuarios	25	A	MA	MA	MB	MA
	[E.2] Errores del administrador	25	A	MA	MA	MB	MA
	[E.15] Alteración accidental de la información	10	MB	B	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[E.19] Fugas de información	50	MB	MB	MA	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	MA	MA	MA	MB	MB
	[A.11] Acceso no autorizado	10	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[A.19] Divulgación de información	50	MB	MB	MA	MB	MB
Acuerdos	[E.1] Errores de los usuarios	25	A	MA	MA	MB	MB
	[E.2] Errores del administrador	25	A	MA	MA	MB	MB
	[E.15] Alteración accidental de la información	10	MB	B	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[E.19] Fugas de información	50	MB	MB	MA	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	MA	MA	MA	MB	MB
	[A.11] Acceso no autorizado	10	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[A.19] Divulgación de información	10	MB	MB	MA	MB	MB

ACTIVO	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Registro de Calificaciones	[E.1] Errores de los usuarios	25	A	MA	MA	MB	MA
	[E.2] Errores del administrador	25	A	MA	MA	MB	MA
	[E.15] Alteración accidental de la información	10	MB	MA	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[E.19] Fugas de información	25	MB	MB	MA	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	MA	MA	MA	MB	MB
	[A.11] Acceso no autorizado	10	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[A.19] Divulgación de información	25	MB	MB	MA	MB	MB
Base de datos de carácter personal	[E.1] Errores de los usuarios	10	MA	MA	MA	MB	MA
	[E.2] Errores del administrador	10	MA	MA	MA	MB	MA
	[E.15] Alteración accidental de la información	10	MB	MA	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[E.19] Fugas de información	25	MB	MB	MA	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	25	MA	MA	MA	MB	MB
	[A.11] Acceso no autorizado	10	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[A.19] Divulgación de información	50	MB	MB	MA	MB	MB

ACTIVO	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Contabilidad del colegio	[E.1] Errores de los usuarios	25	MA	MA	MA	MB	MA
	[E.2] Errores del administrador	25	MA	MA	MA	MB	MA
	[E.15] Alteración accidental de la información	10	MB	MA	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[E.19] Fugas de información	25	MB	MB	MA	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	MA	MA	MA	MB	MB
	[A.11] Acceso no autorizado	10	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[A.19] Divulgación de información	25	MB	MB	MA	MB	MB
Hoja de vida de los Estudiantes	[E.1] Errores de los usuarios	25	MA	MA	MA	MB	MA
	[E.2] Errores del administrador	25	MA	MA	MA	MB	MA
	[E.15] Alteración accidental de la información	10	MB	MA	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[E.19] Fugas de información	25	MB	MB	MA	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	MA	MA	MA	MB	MB
	[A.11] Acceso no autorizado	10	A	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[A.19] Divulgación de información	25	MB	MB	MA	MB	MB

Fuente: Propiedad de los autores

5.1.6.2 [D] DATOS / INFORMACIÓN

En la tabla 34 se hace la evaluación de las amenazas y el impacto que estas tienen sobre el activo [D] DATOS / INFORMACIÓN

Tabla 34. Evaluación de amenazas - [D] DATOS / INFORMACIÓN

ACTIVO	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Calificaciones	[E.1] Errores de los usuarios	25	A	MA	MA	MB	MA
	[E.2] Errores del administrador	25	A	MA	MA	MB	MA
	[E.15] Alteración accidental de la información	10	MB	MA	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[E.19] Fugas de información	25	MB	MB	MA	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	MA	MA	MA	MB	MB
	[A.11] Acceso no autorizado	10	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[A.19] Divulgación de información	25	MB	MB	MA	MB	MB
Contabilidad	[E.1] Errores de los usuarios	25	MA	MA	MA	MB	MA
	[E.2] Errores del administrador	25	MA	MA	MA	MB	MA
	[E.15] Alteración accidental de la información	10	MB	MA	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[E.19] Fugas de información	25	MB	MB	MA	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	MA	MA	MA	MB	MB
	[A.11] Acceso no autorizado	10	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[A.19] Divulgación de información	25	MB	MB	MA	MB	MB
Archivos de actas	[E.1] Errores de los usuarios	25	A	MA	MA	MB	MA
	[E.2] Errores del administrador	25	A	MA	MA	MB	MA
	[E.15] Alteración accidental de la información	10	MB	B	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[E.19] Fugas de información	50	MB	MB	MA	MB	MB

	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	MA	MA	MA	MB	MB
	[A.11] Acceso no autorizado	10	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[A.19] Divulgación de información	10	MB	MB	MA	MB	MB
Resoluciones (Actos administrativos y académicos)	[E.1] Errores de los usuarios	25	A	MA	MA	MB	MA
	[E.2] Errores del administrador	25	A	MA	MA	MB	MA
	[E.15] Alteración accidental de la información	10	MB	B	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[E.19] Fugas de información	50	MB	MB	MA	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	MA	MA	MA	MB	MB
	[A.11] Acceso no autorizado	10	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[A.19] Divulgación de información	10	MB	MB	MA	MB	MB
Observador del alumno	[E.1] Errores de los usuarios	25	MA	MA	MA	MB	MA
	[E.2] Errores del administrador	25	MA	MA	MA	MB	MA
	[E.15] Alteración accidental de la información	10	MB	MA	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[E.19] Fugas de información	25	MB	MB	MA	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	MA	MA	MA	MB	MB
	[A.11] Acceso no autorizado	10	A	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[A.19] Divulgación de información	25	MB	MB	MA	MB	MB

ACTIVO	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Libro de Matricula	[E.1] Errores de los usuarios	10	MA	MA	MA	MB	MA
	[E.2] Errores del administrador	10	MA	MA	MA	MB	MA
	[E.15] Alteración accidental de la información	10	MB	MA	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[E.19] Fugas de información	10	MB	MB	MA	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	MA	MA	MA	MB	MB
	[A.11] Acceso no autorizado	10	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[A.19] Divulgación de información	10	MB	MB	MA	MB	MB
Documentos administrativos	[E.1] Errores de los usuarios	25	A	MA	MA	MB	MA
	[E.2] Errores del administrador	25	A	MA	MA	MB	MA
	[E.15] Alteración accidental de la información	10	MB	B	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[E.19] Fugas de información	50	MB	MB	MA	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	MA	MA	MA	MB	MB
	[A.11] Acceso no autorizado	10	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[A.19] Divulgación de información	10	MB	MB	MA	MB	MB

Fuente: Propiedad de los autores

5.1.6.3 [S] SERVICIOS

A continuación se hace la evaluación de las amenazas y el impacto que estas tienen sobre el activo [S] SERVICIOS ver Tabla 35.

Tabla 35. Evaluación de amenazas - [S] SERVICIOS

ACTIVO	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Diligenciamiento Matriz Chip	[E.1] Errores de los usuarios	10	B	MA	MA	MB	MA
	[E.2] Errores del administrador	10	MA	MA	MA	MB	MA
	[E.9] Errores de [re-]encaminamiento	25	MB	MB	MA	MB	MB
	[E.10] Errores de secuencia	10	MB	MA	MB	MB	MB
	[E.15] Alteración accidental de la información	10	MB	MA	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[E.19] Fugas de información	25	MB	MB	MA	MB	MB
	[E.24] Caída del sistema por agotamiento de recursos	50	MA	MB	MB	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	MA	MA	MA	MB	MB
	[A.7] Uso no previsto	10	MA	MB	MB	MB	MB
	[A.9] [Re-]encaminamiento de mensajes	10	MB	MB	MA	MB	MB
	[A.10] Alteración de secuencia	10	MB	MA	MB	MB	MB
	[A.11] Acceso no autorizado	10	MA	MA	MB	MB	MB
	[A.13] Repudio	10	MB	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[A.19] Divulgación de información	10	MB	MB	MA	MB	MB

Fuente: Propiedad de los autores

5.1.6.4 [SW] SOFTWARE - APLICACIONES INFORMÁTICAS

En la tabla 36 se hace la evaluación de las amenazas y el impacto que estas tienen sobre el activo [SW] SOFTWARE - APLICACIONES INFORMÁTICAS

Tabla 36. . Evaluación de amenazas - [SW] SOFTWARE - APLICACIONES INFORMÁTICAS

ACTIVO	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Sistema operativo Windows 7, Windows 8	[I.5] Avería de origen físico o lógico	25	MA	MA	MB	MB	MA
	[E.1] Errores de los usuarios	50	M	MA	MA	MB	MB
	[E.2] Errores del administrador	10	MA	MA	MA	MB	MB
	[E.8] Difusión de software dañino	75	MA	MA	MA	MB	MB

	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
	[E.9] Errores de [re-]encaminamiento	10	MB	MB	MA	MB	MB
	[E.10] Errores de secuencia	10	MB	MA	MB	MB	MB
	[E.15] Alteración accidental de la información	10	MB	MA	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[E.19] Fugas de información	25	MB	MB	MA	MB	MB
	[E.20] Vulnerabilidades de los programas (software)	50	MA	MA	MA	MB	MB
	[E.21] Errores de mantenimiento / actualización de programas (software)	50	A	MA	MB	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	25	MA	MA	MA	MB	MB
	[A.7] Uso no previsto	10	MA	MA	MA	MB	MB
	[A.8] Difusión de software dañino	75	MA	MA	MA	MB	MB
	[A.9] [Re-]encaminamiento de mensajes	10	MB	MB	MA	MB	MB
	[A.10] Alteración de secuencia	10	MB	MA	MB	MB	MB
	[A.11] Acceso no autorizado	25	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	25	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[A.19] Divulgación de información	25	MB	MB	MA	MB	MB
	[A.22] Manipulación de programas	25	MA	MA	MA	MB	MB
	[A.24] Denegación de servicio	50	MA	MB	MB	MB	MB
Aplicación para el manejo de notas y reportes de los estudiantes.	[I.5] Avería de origen físico o lógico	25	MA	MA	MB	MB	MA
	[E.1] Errores de los usuarios	25	MA	MA	MA	MB	MB
	[E.2] Errores del administrador	25	MA	MA	MA	MB	MB
	[E.8] Difusión de software dañino	75	MA	MA	MA	MB	M
	[E.9] Errores de [re-]encaminamiento	10	MB	MB	MA	MB	MB
	[E.10] Errores de secuencia	25	MB	MA	MB	MB	MB
	[E.15] Alteración accidental de la información	10	MB	MA	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[E.19] Fugas de información	50	MB	MB	MA	MB	MB
	[E.20] Vulnerabilidades de los programas (software)	25	MA	MA	MA	MB	MB

	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
	[E.21] Errores de mantenimiento / actualización de programas (software)	25	MA	MA	MB	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	MA	MA	MA	MB	MB
	[A.7] Uso no previsto	10	MA	MA	MA	MB	MB
	[A.8] Difusión de software dañino	75	MA	MA	MA	MB	M
	[A.9] [Re-]encaminamiento de mensajes	10	MB	MB	MA	MB	MB
	[A.10] Alteración de secuencia	10	MB	MA	MB	MB	MB
	[A.11] Acceso no autorizado	10	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	25	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[A.19] Divulgación de información	25	MB	MB	MA	MB	MB
	[A.22] Manipulación de programas	50	MA	MA	MA	MB	MB
	[A.24] Denegación de servicio	25	MA	MB	MB	MB	MB
Base de datos para almacenar las notas de los estudiantes	[I.5] Avería de origen físico o lógico	25	MA	MB	MB	MB	MA
	[E.1] Errores de los usuarios	25	MA	MA	MA	MB	MA
	[E.2] Errores del administrador	25	MA	MA	MA	MB	MA
	[E.8] Difusión de software dañino	75	MA	MA	MA	MB	MB
	[E.9] Errores de [re-]encaminamiento	10	MB	MB	MA	MB	MB
	[E.10] Errores de secuencia	25	MB	MA	MB	MB	MB
	[E.15] Alteración accidental de la información	10	MB	MA	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[E.19] Fugas de información	50	MB	MB	MA	MB	M
	[E.20] Vulnerabilidades de los programas (software)	25	MA	MA	MA	MB	MB
	[E.21] Errores de mantenimiento / actualización de programas (software)	25	MA	MA	MB	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	MA	MA	MA	MB	MB
	[A.7] Uso no previsto	10	MA	MA	MA	MB	MB
	[A.8] Difusión de software dañino	75	MA	MA	MA	MB	A
	[A.9] [Re-]encaminamiento de mensajes	10	MB	MB	MA	MB	MB

	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
	[A.10] Alteración de secuencia	10	MB	MA	MB	MB	MB
	[A.11] Acceso no autorizado	10	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	25	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MA
	[A.19] Divulgación de información	25	MB	MB	MA	MB	MB
	[A.22] Manipulación de programas	50	MA	MA	MA	MB	MB
	[A.24] Denegación de servicio	25	MA	MB	MB	MB	MB
Office 2013, winrar, Adobe Acrobat Reader.	[I.5] Avería de origen físico o lógico	25	B	MB	MB	MB	MB
	[E.1] Errores de los usuarios	50	MB	MB	MB	MB	MB
	[E.2] Errores del administrador	50	MB	MB	MB	MB	MB
	[E.8] Difusión de software dañino	75	M	B	A	MB	MB
	[E.9] Errores de [re-]encaminamiento	10	MB	MB	MB	MB	MB
	[E.10] Errores de secuencia	10	MB	A	MB	MB	MB
	[E.15] Alteración accidental de la información	25	MB	A	MB	MB	MB
	[E.18] Destrucción de información	25	MB	MB	MB	MB	MB
	[E.19] Fugas de información	25	MB	MB	A	MB	MB
	[E.20] Vulnerabilidades de los programas (software)	50	MA	MA	MA	MB	MB
	[E.21] Errores de mantenimiento / actualización de programas (software)	75	A	A	MB	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	A	A	A	MB	MB
	[A.7] Uso no previsto	50	M	MA	MA	MB	MB
	[A.8] Difusión de software dañino	75	MA	MA	MA	MB	MB
	[A.9] [Re-]encaminamiento de mensajes	10	MB	MB	MB	MB	MB
	[A.10] Alteración de secuencia	10	MB	MB	MB	MB	MB
	[A.11] Acceso no autorizado	75	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	25	MB	A	MB	MB	MB
	[A.18] Destrucción de información	25	MA	MB	MB	MB	MB
	[A.19] Divulgación de información	50	MB	MB	MA	MB	MB
	[A.22] Manipulación de programas	10	MA	MA	MA	MB	MB
	[A.24] Denegación de servicio	25	MA	MB	MB	MB	MB

ACTIVO	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Microsoft Security Essentials.	[I.5] Avería de origen físico o lógico	10	MA	MB	MB	MB	MB
	[E.1] Errores de los usuarios	50	A	M	MA	MB	MB
	[E.2] Errores del administrador	25	MA	MA	MA	MB	MB
	[E.8] Difusión de software dañino	25	A	A	A	MB	MB
	[E.9] Errores de [re-]encaminamiento	10	MB	MB	MB	MB	MB
	[E.10] Errores de secuencia	10	MB	MB	MB	MB	MB
	[E.15] Alteración accidental de la información	10	MB	MB	MB	MB	MB
	[E.18] Destrucción de información	10	A	MB	MB	MB	MB
	[E.19] Fugas de información	50	MB	MB	M	MB	MB
	[E.20] Vulnerabilidades de los programas (software)	25	A	A	A	MB	MB
	[E.21] Errores de mantenimiento / actualización de programas (software)	50	MA	A	MB	MB	MB
	[A.5] Suplantación de la identidad del usuario	25	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	M	MA	A	MB	MB
	[A.7] Uso no previsto	25	B	B	B	MB	MB
	[A.8] Difusión de software dañino	75	A	A	A	MB	MB
	[A.9] [Re-]encaminamiento de mensajes	10	MB	MB	MB	MB	MB
	[A.10] Alteración de secuencia	10	MB	MB	MB	MB	MB
	[A.11] Acceso no autorizado	10	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	25	M	MB	MB	MB	MB
	[A.19] Divulgación de información	50	MB	MB	M	MB	MB
	[A.22] Manipulación de programas	75	B	B	B	MB	MB
	[A.24] Denegación de servicio	25	MA	MB	MB	MB	MB
Java, Cabri-Geom, Crocodile: Deep-Freze, Derive-Matem, Dev-C++ Portable, Gimp, WinCmapTools, MicromundosPro, Photoshop CS4	[I.5] Avería de origen físico o lógico	10	MA	MB	MB	MB	MB
	[E.1] Errores de los usuarios	50	B	B	B	MB	MB
	[E.2] Errores del administrador	25	B	B	B	MB	MB
	[E.8] Difusión de software dañino	10	A	A	A	MB	MB
	[E.9] Errores de [re-]encaminamiento	10	MB	MB	MB	MB	MB
	[E.10] Errores de secuencia	10	MB	MB	MB	MB	MB
	[E.15] Alteración accidental de la información	10	MB	MB	MB	MB	MB

	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Portable_j89, TuxPaint, LEGO DIGITAL DESIGNER, Macromedia_Flash_8_(Portable), MECA NET, Microsoft Mathematics 4.0	[E.18] Destrucción de información	75	B	MB	MB	MB	MB
	[E.19] Fugas de información	10	MB	MB	B	MB	MB
	[E.20] Vulnerabilidades de los programas (software)	25	B	B	B	MB	MB
	[E.21] Errores de mantenimiento / actualización de programas (software)	50	B	B	MB	MB	MB
	[A.5] Suplantación de la identidad del usuario	25	MB	MB	MB	MB	MB
	[A.6] Abuso de privilegios de acceso	10	B	B	B	MB	MB
	[A.7] Uso no previsto	75	B	B	B	MB	MB
	[A.8] Difusión de software dañino	10	A	A	A	MB	MB
	[A.9] [Re-]encaminamiento de mensajes	10	MB	MB	B	MB	MB
	[A.10] Alteración de secuencia	10	MB	MB	MB	MB	MB
	[A.11] Acceso no autorizado	75	MB	MB	MB	MB	MB
	[A.15] Modificación deliberada de la información	25	MB	B	MB	MB	MB
	[A.18] Destrucción de información	50	B	MB	MB	MB	MB
	[A.19] Divulgación de información	75	MB	MB	B	MB	MB
	[A.22] Manipulación de programas	10	B	B	B	MB	MB
	[A.24] Denegación de servicio	25	B	MB	MB	MB	MB

Fuente: Propiedad de los autores

5.1.6.5 [HW] EQUIPAMIENTO INFORMÁTICO (HARDWARE)

En la tabla 37 se hace la evaluación de las amenazas y el impacto que estas tienen sobre el activo [HW] EQUIPAMIENTO INFORMÁTICO (HARDWARE)

Tabla 37. Evaluación de amenazas - [HW] EQUIPAMIENTO INFORMÁTICO (HARDWARE)

ACTIVO	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
72 Equipos de escritorio salas de sistemas	[N.1] Fuego	10	MA	MB	MB	MB	MA
	[N.2] Daños por agua	10	MA	MB	MB	MB	MA
	[N.*] Desastres naturales	10	MA	MB	MB	MB	MA
	[I.1] Fuego	10	MA	MB	MB	MB	MA
	[I.2] Daños por agua	10	MA	MB	MB	MB	MA
	[I.*] Desastres industriales	10	MA	MB	MB	MB	MA
	[I.3] Contaminación mecánica	10	MA	MB	MB	MB	MA
	[I.4] Contaminación electromagnética	10	MA	MB	MB	MB	MA
	[I.5] Avería de origen físico o lógico	10	MA	MB	MB	MB	MA

	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
	[I.6] Corte del suministro eléctrico	50	MA	MB	MB	MB	MA
	[I.7] Condiciones inadecuadas de temperatura o humedad	25	MA	MB	MB	MB	MA
	[I.11] Emanaciones electromagnéticas	10	MB	MB	MA	MB	MA
	[E.2] Errores del administrador	25	A	A	A	MB	MB
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	75	A	MB	MB	MB	MB
	[E.24] Caída del sistema por agotamiento de recursos	50	A	MB	MB	MB	MB
	[E.25] Pérdida de equipos	10	MA	MB	MB	MB	MB
	[A.6] Abuso de privilegios de acceso	25	MA	MA	MA	MB	MB
	[A.7] Uso no previsto	10	B	A	A	MB	MB
	[A.11] Acceso no autorizado	50	A	MA	MB	MB	MB
	[A.23] Manipulación de los equipos	25	M	MB	MA	MB	MB
	[A.24] Denegación de servicio	75	MA	MB	MB	MB	MB
	[A.25] Robo	10	MA	MB	MA	MB	MB
	[A.26] Ataque destructivo	10	MA	MB	MB	MB	MB
12 equipos de escritorio aulas especializadas	[N.1] Fuego	10	MA	MB	MB	MB	MA
	[N.2] Daños por agua	10	MA	MB	MB	MB	MA
	[N.*] Desastres naturales	10	MA	MB	MB	MB	MA
	[I.1] Fuego	10	MA	MB	MB	MB	MA
	[I.2] Daños por agua	10	MA	MB	MB	MB	MA
	[I.*] Desastres industriales	10	MA	MB	MB	MB	MA
	[I.3] Contaminación mecánica	10	MA	MB	MB	MB	MA
	[I.4] Contaminación electromagnética	10	MA	MB	MB	MB	MA
	[I.5] Avería de origen físico o lógico	10	MA	MB	MB	MB	MA
	[I.6] Corte del suministro eléctrico	50	MA	MB	MB	MB	MA
	[I.7] Condiciones inadecuadas de temperatura o humedad	25	MA	MB	MB	MB	MA
	[I.11] Emanaciones electromagnéticas	10	MB	MB	MA	MB	MA
	[E.2] Errores del administrador	25	A	A	A	MB	MB
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	75	A	MB	MB	MB	MB
	[E.24] Caída del sistema por agotamiento de recursos	50	A	MB	MB	MB	MB
	[E.25] Pérdida de equipos	10	MA	MB	MB	MB	MB
	[A.6] Abuso de privilegios de acceso	25	MA	MA	MA	MB	MB
	[A.7] Uso no previsto	10	B	A	A	MB	MB

	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
	[A.11] Acceso no autorizado	50	A	MA	MB	MB	MB
	[A.23] Manipulación de los equipos	25	M	MB	MA	MB	MB
	[A.24] Denegación de servicio	75	MA	MB	MB	MB	MB
	[A.25] Robo	10	MA	MB	MA	MB	MB
	[A.26] Ataque destructivo	10	MA	MB	MB	MB	MB
19 equipos de escritorio zona administrativa	[N.1] Fuego	10	MA	MB	MB	MB	MA
	[N.2] Daños por agua	10	MA	MB	MB	MB	MA
	[N.*] Desastres naturales	10	MA	MB	MB	MB	MA
	[I.1] Fuego	10	MA	MB	MB	MB	MA
	[I.2] Daños por agua	10	MA	MB	MB	MB	MA
	[I.*] Desastres industriales	10	MA	MB	MB	MB	MA
	[I.3] Contaminación mecánica	10	MA	MB	MB	MB	MA
	[I.4] Contaminación electromagnética	10	MA	MB	MB	MB	MA
	[I.5] Avería de origen físico o lógico	10	MA	MB	MB	MB	MA
	[I.6] Corte del suministro eléctrico	50	MA	MB	MB	MB	MA
	[I.7] Condiciones inadecuadas de temperatura o humedad	25	MA	MB	MB	MB	MA
	[I.11] Emanaciones electromagnéticas	10	MB	MB	MA	MB	MB
	[E.2] Errores del administrador	50	MA	MA	MA	MB	MB
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	75	MA	MB	MB	MB	MB
	[E.24] Caída del sistema por agotamiento de recursos	25	MA	MB	MB	MB	MB
	[E.25] Pérdida de equipos	10	MA	MB	MB	MB	MB
	[A.6] Abuso de privilegios de acceso	10	MA	MA	MA	MB	MB
	[A.7] Uso no previsto	25	MA	MA	MA	MB	MB
	[A.11] Acceso no autorizado	10	MA	MA	MB	MB	MB
	[A.23] Manipulación de los equipos	50	MA	MB	MA	MB	MB
	[A.24] Denegación de servicio	25	MA	MB	MB	MB	MA
	[A.25] Robo	10	MA	MB	MA	MB	MB
	[A.26] Ataque destructivo	10	MA	MB	MA	MB	MA
95 Portaltiles aulas especializadas	[N.1] Fuego	10	MA	MB	MB	MB	MA
	[N.2] Daños por agua	10	MA	MB	MB	MB	MA
	[N.*] Desastres naturales	10	MA	MB	MB	MB	MA
	[I.1] Fuego	10	MA	MB	MB	MB	MA
	[I.2] Daños por agua	10	MA	MB	MB	MB	MA
	[I.*] Desastres industriales	10	MA	MB	MB	MB	MA
	[I.3] Contaminación mecánica	10	MA	MB	MB	MB	MA
	[I.4] Contaminación electromagnética	10	MA	MB	MB	MB	MA

	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
	[I.5] Avería de origen físico o lógico	10	MA	MB	MB	MB	MA
	[I.6] Corte del suministro eléctrico	50	MA	MB	MB	MB	MA
	[I.7] Condiciones inadecuadas de temperatura o humedad	25	MA	MB	MB	MB	MA
	[I.11] Emanaciones electromagnéticas	10	MB	MB	MA	MB	MA
	[E.2] Errores del administrador	25	A	A	A	MB	MB
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	75	A	MB	MB	MB	MB
	[E.24] Caída del sistema por agotamiento de recursos	25	A	MB	MB	MB	MB
	[E.25] Pérdida de equipos	10	MA	MB	MB	MB	MB
	[A.6] Abuso de privilegios de acceso	25	MA	MA	MA	MB	MB
	[A.7] Uso no previsto	10	B	A	A	MB	MB
	[A.11] Acceso no autorizado	50	A	MA	MB	MB	MB
	[A.23] Manipulación de los equipos	25	M	MB	MA	MB	MB
	[A.24] Denegación de servicio	75	MA	MB	MB	MB	MB
	[A.25] Robo	10	MA	MB	MA	MB	MB
	[A.26] Ataque destructivo	10	MA	MB	MB	MB	MB
12 antenas de access point	[N.1] Fuego	10	MA	MB	MB	MB	MB
	[N.2] Daños por agua	10	MA	MB	MB	MB	MB
	[N.*] Desastres naturales	10	MA	MB	MB	MB	MB
	[I.1] Fuego	10	MA	MB	MB	MB	MB
	[I.2] Daños por agua	10	MA	MB	MB	MB	MB
	[I.*] Desastres industriales	10	MA	MB	MB	MB	MB
	[I.3] Contaminación mecánica	10	MA	MB	MB	MB	MB
	[I.4] Contaminación electromagnética	10	MA	MB	MB	MB	MB
	[I.5] Avería de origen físico o lógico	10	MA	MB	MB	MB	MB
	[I.6] Corte del suministro eléctrico	50	MA	MB	MB	MB	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	25	MA	MB	MB	MB	MB
	[I.11] Emanaciones electromagnéticas	10	MB	MB	MA	MB	MB
	[E.2] Errores del administrador	25	A	MA	MA	MB	MB
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	75	A	MB	MB	MB	MB
	[E.24] Caída del sistema por agotamiento de recursos	25	MA	MB	MB	MB	MB
	[E.25] Pérdida de equipos	10	MA	MB	MB	MB	MB
	[A.6] Abuso de privilegios de acceso	25	MA	A	A	MB	MB

	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
	[A.7] Uso no previsto	10	MA	B	B	MB	MB
	[A.11] Acceso no autorizado	50	A	A	MB	MB	MB
	[A.23] Manipulación de los equipos	10	M	MB	M	MB	MB
	[A.24] Denegación de servicio	75	MA	MB	MB	MB	MB
	[A.25] Robo	10	MA	MB	MA	MB	MB
	[A.26] Ataque destructivo	10	MA	MB	MB	MB	MB
4 switch 24 puertos	[N.1] Fuego	10	MA	MB	MB	MB	MB
	[N.2] Daños por agua	10	MA	MB	MB	MB	MB
	[N.*] Desastres naturales	10	MA	MB	MB	MB	MB
	[I.1] Fuego	10	MA	MB	MB	MB	MB
	[I.2] Daños por agua	10	MA	MB	MB	MB	MB
	[I.*] Desastres industriales	10	MA	MB	MB	MB	MB
	[I.3] Contaminación mecánica	10	MA	MB	MB	MB	MB
	[I.4] Contaminación electromagnética	10	MA	MB	MB	MB	MB
	[I.5] Avería de origen físico o lógico	10	MA	MB	MB	MB	MB
	[I.6] Corte del suministro eléctrico	50	MA	MB	MB	MB	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	25	MA	MB	MB	MB	MB
	[I.11] Emanaciones electromagnéticas	10	MA	MB	MA	MB	MB
	[E.2] Errores del administrador	25	A	MA	MA	MB	MB
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	75	A	MB	MB	MB	MB
	[E.24] Caída del sistema por agotamiento de recursos	10	MA	MB	MB	MB	MB
	[E.25] Pérdida de equipos	10	MA	MB	MB	MB	MB
	[A.6] Abuso de privilegios de acceso	25	MA	A	A	MB	MB
	[A.7] Uso no previsto	10	MA	B	B	MB	MB
	[A.11] Acceso no autorizado	50	A	A	MB	MB	MB
	[A.23] Manipulación de los equipos	10	M	MB	M	MB	MB
	[A.24] Denegación de servicio	75	MA	MB	MB	MB	MB
	[A.25] Robo	10	MA	MB	MA	MB	MB
	[A.26] Ataque destructivo	10	MA	MB	MB	MB	MB
Router CISCO 2900 Series.	[N.1] Fuego	10	MA	MB	MB	MB	MB
	[N.2] Daños por agua	10	MA	MB	MB	MB	MB
	[N.*] Desastres naturales	10	MA	MB	MB	MB	MB
	[I.1] Fuego	10	MA	MB	MB	MB	MB
	[I.2] Daños por agua	10	MA	MB	MB	MB	MB
	[I.*] Desastres industriales	10	MA	MB	MB	MB	MB
	[I.3] Contaminación mecánica	10	MA	MB	MB	MB	MB

	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
	[I.4] Contaminación electromagnética	10	MA	MB	MB	MB	MB
	[I.5] Avería de origen físico o lógico	10	MA	MB	MB	MB	MB
	[I.6] Corte del suministro eléctrico	50	MA	MB	MB	MB	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	25	MA	MB	MB	MB	MB
	[I.11] Emanaciones electromagnéticas	10	MA	MB	MA	MB	MB
	[E.2] Errores del administrador	25	A	MA	MA	MB	MB
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	75	A	MB	MB	MB	MB
	[E.24] Caída del sistema por agotamiento de recursos	25	MA	MB	MB	MB	MB
	[E.25] Pérdida de equipos	10	MA	MB	MB	MB	MB
	[A.6] Abuso de privilegios de acceso	25	MA	A	A	MB	MB
	[A.7] Uso no previsto	10	MA	B	B	MB	MB
	[A.11] Acceso no autorizado	50	A	A	MB	MB	MB
	[A.23] Manipulación de los equipos	10	M	MB	M	MB	MB
	[A.24] Denegación de servicio	75	MA	MB	MB	MB	MB
	[A.25] Robo	10	MA	MB	MA	MB	MB
	[A.26] Ataque destructivo	10	MA	MB	MB	MB	MB
2 Impresoras salas de sistemas	[N.1] Fuego	10	MA	MB	MB	MB	MB
	[N.2] Daños por agua	10	MA	MB	MB	MB	MB
	[N.*] Desastres naturales	10	MA	MB	MB	MB	MB
	[I.1] Fuego	10	MA	MB	MB	MB	MB
	[I.2] Daños por agua	10	MA	MB	MB	MB	MB
	[I.*] Desastres industriales	10	MA	MB	MB	MB	MB
	[I.3] Contaminación mecánica	10	MA	MB	MB	MB	MB
	[I.4] Contaminación electromagnética	10	MA	MB	MB	MB	MB
	[I.5] Avería de origen físico o lógico	10	MA	MB	MB	MB	MB
	[I.6] Corte del suministro eléctrico	50	MA	MB	MB	MB	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	25	MA	MB	MB	MB	MB
	[I.11] Emanaciones electromagnéticas	10	MA	MB	MB	MB	MB
	[E.2] Errores del administrador	25	B	MB	MB	MB	MB
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	75	A	MB	MB	MB	MB
	[E.24] Caída del sistema por agotamiento de recursos	10	MA	MB	MB	MB	MB
	[E.25] Pérdida de equipos	10	MA	MB	MB	MB	MB

	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
	[A.6] Abuso de privilegios de acceso	25	A	MB	MB	MB	MB
	[A.7] Uso no previsto	10	A	MB	MB	MB	MB
	[A.11] Acceso no autorizado	50	A	MB	MB	MB	MB
	[A.23] Manipulación de los equipos	10	M	MB	MB	MB	MB
	[A.24] Denegación de servicio	75	A	MB	MB	MB	MB
	[A.25] Robo	10	MA	MB	MB	MB	MB
	[A.26] Ataque destructivo	10	MA	MB	MB	MB	MB
2 impresoras de multifunción (zona administrativa) 1 impresora chorro de tinta (zona administrativa) 1 impresora inalambrica (zona administrativa)	[N.1] Fuego	10	MA	MB	MB	MB	MB
	[N.2] Daños por agua	10	MA	MB	MB	MB	MB
	[N.*] Desastres naturales	10	MA	MB	MB	MB	MB
	[I.1] Fuego	10	MA	MB	MB	MB	MB
	[I.2] Daños por agua	10	MA	MB	MB	MB	MB
	[I.*] Desastres industriales	10	MA	MB	MB	MB	MB
	[I.3] Contaminación mecánica	10	MA	MB	MB	MB	MB
	[I.4] Contaminación electromagnética	10	MA	MB	MB	MB	MB
	[I.5] Avería de origen físico o lógico	10	MA	MB	MB	MB	MB
	[I.6] Corte del suministro eléctrico	50	MA	MB	MB	MB	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	25	MA	MB	MB	MB	MB
	[I.11] Emanaciones electromagnéticas	10	MA	MB	MB	MB	MB
	[E.2] Errores del administrador	25	B	MB	MB	MB	MB
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	75	A	MB	MB	MB	MB
	[E.24] Caída del sistema por agotamiento de recursos	10	MA	MB	MB	MB	MB
	[E.25] Pérdida de equipos	10	MA	MB	MB	MB	MB
	[A.6] Abuso de privilegios de acceso	25	A	MB	MB	MB	MB
	[A.7] Uso no previsto	10	A	MB	MB	MB	MB
	[A.11] Acceso no autorizado	50	A	MB	MB	MB	MB
	[A.23] Manipulación de los equipos	10	M	MB	MB	MB	MB
	[A.24] Denegación de servicio	75	A	MB	MB	MB	MB
	[A.25] Robo	10	MA	MB	MB	MB	MB
	[A.26] Ataque destructivo	10	MA	MB	MB	MB	MB

Fuente: Propiedad de los autores

5.1.6.6 [COM] REDES DE COMUNICACIONES

En la tabla 39 se hace la evaluación de las amenazas y el impacto que estas tienen sobre el activo [COM] REDES DE COMUNICACIONES

Tabla 38. Evaluación de amenazas - [COM] REDES DE COMUNICACIONES

ACTIVO	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Acceso telefónico ETB	[I.8] Fallo de servicios de comunicaciones	25	MA	MB	MB	MB	MB
	[E.2] Errores del administrador	10	MA	MB	MB	MB	MB
	[E.9] Errores de [re-]encaminamiento	10	MB	MB	A	MB	MB
	[E.10] Errores de secuencia	10	MB	MB	MB	MB	MB
	[E.15] Alteración accidental de la información	10	MB	MB	MB	MB	MB
	[E.18] Destrucción de información	10	MB	MB	MB	MB	MB
	[E.19] Fugas de información	10	MB	MB	MA	MB	MB
	[E.24] Caída del sistema por agotamiento de recursos	10	MA	MB	MB	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	A	MA	MA	MB	MB
	[A.7] Uso no previsto	10	M	MA	MA	MB	MB
	[A.9] [Re-]encaminamiento de mensajes	10	MB	MB	MA	MB	MB
	[A.10] Alteración de secuencia	10	MB	M	MB	MB	MB
	[A.11] Acceso no autorizado	10	MA	A	MB	MB	MB
	[A.12] Análisis de tráfico	25	MB	MB	A	MB	MB
	[A.14] Interceptación de información (escucha)	50	MB	MB	MA	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.19] Divulgación de información	10	MB	MB	MA	MB	MB
	[A.24] Denegación de servicio	25	MA	MB	MB	MB	MB
Red Lan	[I.8] Fallo de servicios de comunicaciones	10	MA	MB	MB	MB	MB
	[E.2] Errores del administrador	10	M	MA	MA	MB	MB
	[E.9] Errores de [re-]encaminamiento	10	MB	MB	MA	MB	MB
	[E.10] Errores de secuencia	10	MB	B	MB	MB	MB
	[E.15] Alteración accidental de la información	10	MB	MA	MB	MB	MB
	[E.18] Destrucción de información	10	A	MB	MB	MB	MB
	[E.19] Fugas de información	10	MB	MB	MA	MB	MB
	[E.24] Caída del sistema por agotamiento de recursos	25	MA	MB	MB	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	MA	MA	MA	MB	MB

	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
	[A.7] Uso no previsto	25	M	MA	MA	MB	MB
	[A.9] [Re-]encaminamiento de mensajes	10	MB	MB	MA	MB	MB
	[A.10] Alteración de secuencia	10	MB	MA	MB	MB	MB
	[A.11] Acceso no autorizado	10	B	MA	MB	MB	MB
	[A.12] Análisis de tráfico	25	MB	MB	MA	MB	MB
	[A.14] Interceptación de información (escucha)	10	MB	MB	MA	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.19] Divulgación de información	10	MB	MB	MA	MB	MB
	[A.24] Denegación de servicio	25	MA	MB	MB	MB	MB
Red Inalámbrica	[I.8] Fallo de servicios de comunicaciones	10	MA	MB	MB	MB	MB
	[E.2] Errores del administrador	10	MA	MA	MA	MB	MB
	[E.9] Errores de [re-]encaminamiento	10	MB	MB	MA	MB	MB
	[E.10] Errores de secuencia	10	MB	MA	MB	MB	MB
	[E.15] Alteración accidental de la información	10	MB	MA	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MB
	[E.19] Fugas de información	10	MB	MB	MA	MB	MB
	[E.24] Caída del sistema por agotamiento de recursos	25	MA	MB	MB	MB	MB
	[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
	[A.6] Abuso de privilegios de acceso	10	MA	MA	MA	MB	MB
	[A.7] Uso no previsto	25	M	MA	MA	MB	MB
	[A.9] [Re-]encaminamiento de mensajes	10	MB	MB	MA	MB	MB
	[A.10] Alteración de secuencia	10	MB	MA	MB	MB	MB
	[A.11] Acceso no autorizado	10	B	MA	MB	MB	MB
	[A.12] Análisis de tráfico	25	MB	MB	MA	MB	MB
	[A.14] Interceptación de información (escucha)	10	MB	MB	MA	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.19] Divulgación de información	10	MB	MB	MA	MB	MB
	[A.24] Denegación de servicio	25	MA	MB	MB	MB	MB
ETB	[I.8] Fallo de servicios de comunicaciones	50	MA	MB	MB	MB	MB
	[E.2] Errores del administrador	10	MA	MA	MA	MB	MB
	[E.9] Errores de [re-]encaminamiento	10	MB	MB	MA	MB	MB
	[E.10] Errores de secuencia	10	MB	MA	MB	MB	MB

AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
[E.15] Alteración accidental de la información	10	MB	MA	MB	MB	MB
[E.18] Destrucción de información	10	MA	MB	MB	MB	MB
[E.19] Fugas de información	10	MB	MB	MA	MB	MB
[E.24] Caída del sistema por agotamiento de recursos	25	MA	MB	MB	MB	MB
[A.5] Suplantación de la identidad del usuario	10	MB	MA	MA	MA	MB
[A.6] Abuso de privilegios de acceso	10	MA	MA	MA	MB	MB
[A.7] Uso no previsto	25	M	MA	MA	MB	MB
[A.9] [Re-]encaminamiento de mensajes	10	MB	MB	MA	MB	MB
[A.10] Alteración de secuencia	10	MB	MA	MB	MB	MB
[A.11] Acceso no autorizado	10	B	MA	MB	MB	MB
[A.12] Análisis de tráfico	25	MB	MB	MA	MB	MB
[A.14] Interceptación de información (escucha)	10	MB	MB	MA	MB	MB
[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
[A.19] Divulgación de información	10	MB	MB	MA	MB	MB
[A.24] Denegación de servicio	25	MA	MB	MB	MB	MB

Fuente: Propiedad de los autores

5.1.6.7 [MEDIA] SOPORTES DE INFORMACIÓN

En la tabla 39 se hace la evaluación de las amenazas y el impacto que estas tienen sobre el activo [MEDIA] SOPORTES DE INFORMACIÓN

Tabla 39. Evaluación de amenazas - [INFO] INFORMACIÓN

ACTIVO	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Actas, resoluciones, observador de los estudiantes, agenda telefónica, fotografías de los estudiantes por cursos, Soporte de contabilidad.	[N.1] Fuego	10	MA	MA	MB	MB	MA
	[N.2] Daños por agua	10	MA	MA	MB	MB	MA
	[N.*] Desastres naturales	10	MA	MA	MB	MB	MA
	[I.1] Fuego	10	MA	MA	MB	MB	MA
	[I.2] Daños por agua	10	MA	MA	MB	MB	MA
	[I.*] Desastres industriales	10	MA	MA	MB	MB	MA
	[I.3] Contaminación mecánica	10	MB	MB	MB	MB	MB
	[I.4] Contaminación electromagnética	10	MB	MB	MB	MB	MB
	[I.5] Avería de origen físico o lógico	10	MA	MB	MB	MB	MA
	[I.6] Corte del suministro eléctrico	10	MB	MB	MB	MB	MB

ACTIVO	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
	[I.7] Condiciones inadecuadas de temperatura o humedad	25	MA	MB	MB	MB	MB
	[I.11] Emanaciones electromagnéticas	10	MB	MB	MB	MB	MB
	[E.1] Errores de los usuarios	10	MB	MB	MB	MB	MB
	[E.2] Errores del administrador	10	MB	MB	MB	MB	MB
	[E.15] Alteración accidental de la información	10	MB	MB	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MB
	[E.19] Fugas de información	50	MA	MB	MA	MB	MA
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	50	MB	MB	MB	MB	MB
	[E.25] Pérdida de equipos	25	MA	MB	MB	MB	MB
	[A.7] Uso no previsto	10	M	MA	MA	MB	MA
	[A.11] Acceso no autorizado	25	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MB
	[A.19] Divulgación de información	10	MB	MB	MA	MB	MB
	[A.23] Manipulación de los equipos	10	MA	MB	MA	MB	MA
	[A.25] Robo	10	MA	MB	MA	MB	MA
	[A.26] Ataque destructivo	10	MA	MB	MB	MB	MA
Copia de seguridad, documentos	[N.1] Fuego	10	MA	MA	MB	MB	MA
	[N.2] Daños por agua	10	MA	MA	MB	MB	MA
	[N.*] Desastres naturales	10	MA	MA	MB	MB	MA
	[I.1] Fuego	10	MA	MA	MB	MB	MA
	[I.2] Daños por agua	10	MA	MA	MB	MB	MA
	[I.*] Desastres industriales	10	MA	MA	MB	MB	MA
	[I.3] Contaminación mecánica	10	MB	MB	MB	MB	MB
	[I.4] Contaminación electromagnética	10	MB	MB	MB	MB	MB
	[I.5] Avería de origen físico o lógico	10	MA	MB	MB	MB	MA
	[I.6] Corte del suministro eléctrico	10	MB	MB	MB	MB	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	25	MA	MB	MB	MB	MB
	[I.11] Emanaciones electromagnéticas	10	MB	MB	MB	MB	MB
	[E.1] Errores de los usuarios	10	MB	MB	MB	MB	MB
	[E.2] Errores del administrador	10	MB	MB	MB	MB	MB
	[E.15] Alteración accidental de la información	10	MB	MB	MB	MB	MB

	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MB
	[E.19] Fugas de información	50	MA	MB	MA	MB	MA
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	50	MB	MB	MB	MB	MB
	[E.25] Pérdida de equipos	25	MA	MB	MB	MB	MB
	[A.7] Uso no previsto	10	M	MA	MA	MB	MA
	[A.11] Acceso no autorizado	25	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MB
	[A.19] Divulgación de información	10	MB	MB	MA	MB	MB
	[A.23] Manipulación de los equipos	10	MA	MB	MA	MB	MA
	[A.25] Robo	10	MA	MB	MA	MB	MA
	[A.26] Ataque destructivo	10	MA	MB	MB	MB	MA
Proyecto educativo institucional, actas institucionales, documentos institucionales	[N.1] Fuego	10	MA	MA	MB	MB	MA
	[N.2] Daños por agua	10	MA	MA	MB	MB	MA
	[N.*] Desastres naturales	10	MA	MA	MB	MB	MA
	[I.1] Fuego	10	MA	MA	MB	MB	MA
	[I.2] Daños por agua	10	MA	MA	MB	MB	MA
	[I.*] Desastres industriales	10	MA	MA	MB	MB	MA
	[I.3] Contaminación mecánica	10	MB	MB	MB	MB	MB
	[I.4] Contaminación electromagnética	10	MB	MB	MB	MB	MB
	[I.5] Avería de origen físico o lógico	10	MA	MB	MB	MB	MA
	[I.6] Corte del suministro eléctrico	10	MB	MB	MB	MB	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	25	MA	MB	MB	MB	MB
	[I.11] Emanaciones electromagnéticas	10	MB	MB	MB	MB	MB
	[E.1] Errores de los usuarios	10	MB	MB	MB	MB	MB
	[E.2] Errores del administrador	10	MB	MB	MB	MB	MB
	[E.15] Alteración accidental de la información	10	MB	MB	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MB
	[E.19] Fugas de información	50	MA	MB	MA	MB	MA
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	50	MB	MB	MB	MB	MB
	[E.25] Pérdida de equipos	25	MA	MB	MB	MB	MB
	[A.7] Uso no previsto	10	M	MA	MA	MB	MA
	[A.11] Acceso no autorizado	25	MA	MA	MB	MB	MB

	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MB
	[A.19] Divulgación de información	10	MB	MB	MA	MB	MB
	[A.23] Manipulación de los equipos	10	MA	MB	MA	MB	MA
	[A.25] Robo	10	MA	MB	MA	MB	MA
	[A.26] Ataque destructivo	10	MA	MB	MB	MB	MA
Copia de Seguridad notas	[N.1] Fuego	10	MA	MA	MB	MB	MA
	[N.2] Daños por agua	10	MA	MA	MB	MB	MA
	[N.*] Desastres naturales	10	MA	MA	MB	MB	MA
	[I.1] Fuego	10	MA	MA	MB	MB	MA
	[I.2] Daños por agua	10	MA	MA	MB	MB	MA
	[I.*] Desastres industriales	10	MA	MA	MB	MB	MA
	[I.3] Contaminación mecánica	10	MB	MB	MB	MB	MB
	[I.4] Contaminación electromagnética	10	MB	MB	MB	MB	MB
	[I.5] Avería de origen físico o lógico	10	MA	MB	MB	MB	MA
	[I.6] Corte del suministro eléctrico	10	MB	MB	MB	MB	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	25	MA	MB	MB	MB	MB
	[I.11] Emanaciones electromagnéticas	10	MB	MB	MB	MB	MB
	[E.1] Errores de los usuarios	10	MB	MB	MB	MB	MB
	[E.2] Errores del administrador	10	MB	MB	MB	MB	MB
	[E.15] Alteración accidental de la información	10	MB	MB	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MB
	[E.19] Fugas de información	50	MA	MB	MA	MB	MA
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	50	MB	MB	MB	MB	MB
	[E.25] Pérdida de equipos	25	MA	MB	MB	MB	MB
	[A.7] Uso no previsto	10	M	MA	MA	MB	MA
	[A.11] Acceso no autorizado	25	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MB
	[A.19] Divulgación de información	10	MB	MB	MA	MB	MB
	[A.23] Manipulación de los equipos	10	MA	MB	MA	MB	MA
	[A.25] Robo	10	MA	MB	MA	MB	MA

	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
	[A.26] Ataque destructivo	10	MA	MB	MB	MB	MA
Actas, resoluciones, observador del estudiantes, agenda telefónicas, fotografías de los estudiantes por cursos, Soporte de contabilidad, boletines, informes académicos, constancias, etc.	[N.1] Fuego	10	MA	MA	MB	MB	MA
	[N.2] Daños por agua	10	MA	MA	MB	MB	MA
	[N.*] Desastres naturales	10	MA	MA	MB	MB	MA
	[I.1] Fuego	10	MA	MA	MB	MB	MA
	[I.2] Daños por agua	10	MA	MA	MB	MB	MA
	[I.*] Desastres industriales	10	MA	MA	MB	MB	MA
	[I.3] Contaminación mecánica	10	MB	MB	MB	MB	MB
	[I.4] Contaminación electromagnética	10	MB	MB	MB	MB	MB
	[I.5] Avería de origen físico o lógico	10	MA	MB	MB	MB	MA
	[I.6] Corte del suministro eléctrico	10	MB	MB	MB	MB	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	25	MA	MB	MB	MB	MB
	[I.11] Emanaciones electromagnéticas	10	MB	MB	MB	MB	MB
	[E.1] Errores de los usuarios	10	MB	MB	MB	MB	MB
	[E.2] Errores del administrador	10	MB	MB	MB	MB	MB
	[E.15] Alteración accidental de la información	10	MB	MB	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MB
	[E.19] Fugas de información	50	MA	MB	MA	MB	MA
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	50	MB	MB	MB	MB	MB
	[E.25] Pérdida de equipos	25	MA	MB	MB	MB	MB
	[A.7] Uso no previsto	10	M	MA	MA	MB	MA
	[A.11] Acceso no autorizado	25	MA	MA	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MA	MB	MB	MB
	[A.18] Destrucción de información	10	MA	MB	MB	MB	MB
	[A.19] Divulgación de información	10	MB	MB	MA	MB	MB
	[A.23] Manipulación de los equipos	10	MA	MB	MA	MB	MA
	[A.25] Robo	10	MA	MB	MA	MB	MA
	[A.26] Ataque destructivo	10	MA	MB	MB	MB	MA

Fuente: Propiedad de los autores

5.1.6.8 [AUX] EQUIPAMIENTO AUXILIAR

En la tabla 40 se hace la evaluación de las amenazas y el impacto que estas tienen sobre el activo [AUX] EQUIPAMIENTO AUXILIAR

Tabla 40. Evaluación de amenazas - [AUX] EQUIPAMIENTO AUXILIAR

ACTIVO	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Instalaciones para el suministro de energía	[N.1] Fuego	10	MA	MB	MB	MB	MB
	[N.2] Daños por agua	10	MA	MB	MB	MB	MB
	[N.*] Desastres naturales	10	MA	MB	MB	MB	MB
	[I.1] Fuego	10	MA	MB	MB	MB	MB
	[I.2] Daños por agua	10	MA	MB	MB	MB	MB
	[I.*] Desastres industriales	10	MA	MB	MB	MB	MB
	[I.3] Contaminación mecánica	10	MA	MB	MB	MB	MB
	[I.4] Contaminación electromagnética	10	MA	MB	MB	MB	MB
	[I.5] Avería de origen físico o lógico	10	M	MB	MB	MB	MB
	[I.6] Corte del suministro eléctrico	25	MA	MB	MB	MB	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	50	MA	MB	MB	MB	MB
	[I.9] Interrupción de otros servicios y suministros esenciales	50	MA	MB	MB	MB	MB
	[I.10] Degradación de los soportes de almacenamiento de la información	50	MA	MB	MB	MB	MB
	[I.11] Emanaciones electromagnéticas	10	MA	MB	MA	MB	MB
	[E.15] Alteración accidental de la información	10	MA	A	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MB
	[E.19] Fugas de información	10	M	MB	M	MB	MB
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	25	M	MB	MB	MB	MB
	[E.25] Pérdida de equipos	10	MA	MB	MB	MB	MB
	[A.7] Uso no previsto	10	M	M	M	MB	MB
	[A.11] Acceso no autorizado	25	B	B	MB	MB	MB
	[A.23] Manipulación de los equipos	10	A	MB	A	MB	MB
	[A.25] Robo	10	MA	MB	MA	MB	MB
	[A.26] Ataque destructivo	10	MA	MB	MB	MB	MB
rack, armarios, archivadores, mesas, muebles, etc	[N.1] Fuego	10	MA	MB	MB	MB	MB
	[N.2] Daños por agua	10	MA	MB	MB	MB	MB
	[N.*] Desastres naturales	10	MA	MB	MB	MB	MB
	[I.1] Fuego	10	MA	MB	MB	MB	MB
	[I.2] Daños por agua	10	MA	MB	MB	MB	MB
	[I.*] Desastres industriales	10	MA	MB	MB	MB	MB
	[I.3] Contaminación mecánica	10	MA	MB	MB	MB	MB
	[I.4] Contaminación electromagnética	10	MA	MB	MB	MB	MB

ACTIVO	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
	[I.5] Avería de origen físico o lógico	10	M	MB	MB	MB	MB
	[I.6] Corte del suministro eléctrico	25	MA	MB	MB	MB	MB
	[I.7] Condiciones inadecuadas de temperatura o humedad	50	MA	MB	MB	MB	MB
	[I.9] Interrupción de otros servicios y suministros esenciales	50	MA	MB	MB	MB	MB
	[I.10] Degradación de los soportes de almacenamiento de la información	50	MA	MB	MB	MB	MB
	[I.11] Emanaciones electromagnéticas	10	MA	MB	MA	MB	MB
	[E.15] Alteración accidental de la información	10	MA	A	MB	MB	MB
	[E.18] Destrucción de información	10	MA	MB	MB	MB	MB
	[E.19] Fugas de información	10	M	MB	M	MB	MB
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	25	M	MB	MB	MB	MB
	[E.25] Pérdida de equipos	10	MA	MB	MB	MB	MB
	[A.7] Uso no previsto	10	M	M	M	MB	MB
	[A.11] Acceso no autorizado	25	B	B	MB	MB	MB
	[A.23] Manipulación de los equipos	10	A	MB	A	MB	MB
	[A.25] Robo	10	MA	MB	MA	MB	MB
	[A.26] Ataque destructivo	10	MA	MB	MB	MB	MB

Fuente: Propiedad de los autores

5.1.6.9 [L] INSTALACIONES

En la tabla 41 se hace la evaluación de las amenazas y el impacto que estas tienen sobre el activo [L] INSTALACIONES

Tabla 41. Evaluación de amenazas - [L] INSTALACIONES

ACTIVO	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Edificio sede colegio Luis Carlos Galán Sarmiento	[N.1] Fuego	10	A	MB	MB	MB	MB
	[N.2] Daños por agua	10	M	MB	MB	MB	MB
	[N.*] Desastres naturales	10	MA	MB	MB	MB	MB
	[I.1] Fuego	10	A	MB	MB	MB	MB
	[I.2] Daños por agua	10	M	MB	MB	MB	MB
	[I.*] Desastres industriales	10	MA	MB	MB	MB	MB
	[I.11] Emanaciones electromagnéticas	10	MB	MB	MB	MB	MB
	[E.15] Alteración accidental de la información	10	MB	MB	MB	MB	MB
	[E.18] Destrucción de información	10	MB	MB	MB	MB	MB

ACTIVO	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
	[E.19] Fugas de información	10	MB	MB	MB	MB	MB
	[A.7] Uso no previsto	10	M	MB	MB	MB	MB
	[A.11] Acceso no autorizado	10	B	MB	MB	MB	MB
	[A.15] Modificación deliberada de la información	10	MB	MB	MB	MB	MB
	[A.18] Destrucción de información	10	MB	MB	MB	MB	MB
	[A.19] Divulgación de información	10	MB	MB	MB	MB	MB
	[A.26] Ataque destructivo	10	MA	MB	MB	MB	MB
	[A.27] Ocupación enemiga	10	MA	MB	MA	MB	MB

Fuente: Propiedad de los autores

5.1.6.10 [P] PERSONAL

En la tabla 42 se hace la evaluación de las amenazas y el impacto que estas tienen sobre el activo [P] PERSONAL

Tabla 42. Evaluación de amenazas - [P] PERSONAL

ACTIVO	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
REDP	[E.7] Deficiencias en la organización	10	MA	MB	MB	MB	MB
	[E.19] Fugas de información	50	MA	MB	MA	MB	MB
	[E.28] Indisponibilidad del personal	25	B	MB	MB	MB	MB
	[A.28] Indisponibilidad del personal	25	B	MB	MB	MB	MB
	[A.29] Extorsión	10	B	MA	MA	MB	MB
	[A.30] Ingeniería social (picaresca)	50	M	MA	MA	MB	MB
Administrativos, docentes	[E.7] Deficiencias en la organización	25	MA	MB	MB	MB	MB
	[E.19] Fugas de información	50	MA	MB	MA	MB	MB
	[E.28] Indisponibilidad del personal	25	M	MB	MB	MB	MB
	[A.28] Indisponibilidad del personal	25	M	MB	MB	MB	MB
	[A.29] Extorsión	10	B	MA	MA	MB	MB
	[A.30] Ingeniería social (picaresca)	50	M	MA	MA	MB	MB
Docente de media Integrada e Informática	[E.7] Deficiencias en la organización	25	MA	MB	MB	MB	MB
	[E.19] Fugas de información	50	MA	MB	MA	MB	MB
	[E.28] Indisponibilidad del personal	25	M	MB	MB	MB	MB
	[A.28] Indisponibilidad del personal	25	M	MB	MB	MB	MB
	[A.29] Extorsión	10	B	MA	MA	MB	MB

ACTIVO	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
	[A.30] Ingeniería social (picaresca)	50	M	MA	MA	MB	MB
ETB	[E.7] Deficiencias en la organización	10	MA	MB	MB	MB	MB
	[E.19] Fugas de información	50	MA	MB	MA	MB	MB
	[E.28] Indisponibilidad del personal	25	M	MB	MB	MB	MB
	[A.28] Indisponibilidad del personal	25	M	MB	MB	MB	MB
	[A.29] Extorsión	10	B	MA	MA	MB	MB
	[A.30] Ingeniería social (picaresca)	50	M	MA	MA	MB	MB

Fuente: Propiedad de los autores

5.2 ANALISIS DE RIESGOS

5.2.1 Impacto Potencial

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema[70].

5.2.2 Riesgo Potencial

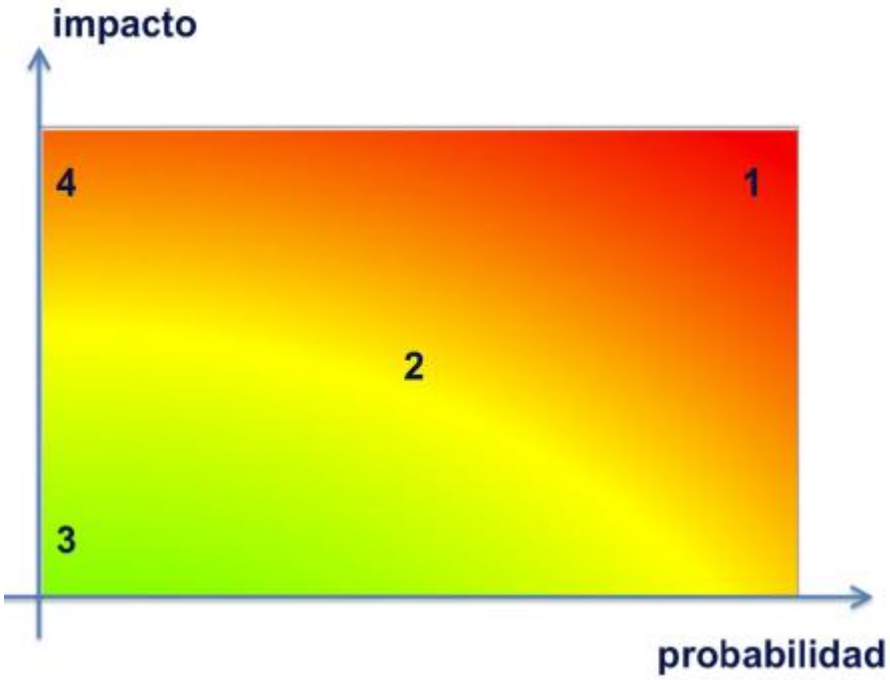
Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia[71].

En la figura 10 se puede observar como el riesgo crece con el impacto y con la probabilidad, por lo tanto el riesgo lo podemos calcular como:

$$\boldsymbol{Riesgo = Probabilidad\ x\ Impacto}$$

[70] MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método, p. 28.
[71] Ibíd. p. 29-30.

Figura 10. Riesgo en función del impacto y la probabilidad



Fuente: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método, p. 30.

De acuerdo a la figura XX podemos identificar las zonas tener en cuenta en el tratamiento del riesgo.
ZONA 1 – riesgos muy probables y de muy alto impacto

ZONA 2 – franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo

ZONA 3 – riesgos improbables y de bajo impacto

ZONA 4 – riesgos improbables pero de muy alto impacto

5.2.3 Criterios de Evaluación

La escala de valoración se determina de acuerdo a las zonas de tratamiento del riesgo, en una escala cualitativa como se muestra en la tabla 44 y 45.

Tabla 43. Estimación cualitativa del riesgo

RIESGO		**PROBABILIDAD**				
		MB	B	M	A	MA
IMPACTO	MA	M	M	A	MA	MA
	A	B	M	M	A	MA
	M	B	B	M	M	A
	B	MB	B	B	M	M
	MB	MB	MB	B	B	M

Fuente: Propiedad de los autores

Tabla 44. Riesgo Potencial

IMPACTO	PROBABILIDAD	RIESGO
MA: MUY ALTO	MA: INSEGURO	MA: CRITICO
A: ALTO	A: PROBABLE	A: IMPORTANTE
M: MEDIO	M: POSIBLE	M: APRECIABLE
B: BAJO	B: POCO PROBABLE	B: BAJO
MB: MUY BAJO	MB: MUY RARO	MB: DESPRECIABLE

Fuente: Propiedad de los autores

5.2.4 **Evaluación del riesgo**

En la Tabla 46 se encuentra la evaluación de riesgo potencial a los activos de la información del colegio Luis Carlos Galán Sarmiento de acuerdo al impacto de las amenazas de manera cualitativa.

Tabla 45. Evaluación de Riesgos

TIPO DE ACTIVO	CÓDIGO DE ACTIVO	DESCRIPCIÓN	IMPACTO	PROBABILIDAD	RIESGO
[essencial] Activos Esenciales	[adm]	Contratos	M	A	M
		Acuerdos	M	A	M
	[vr]	Registro de Calificaciones	A	M	M
	[per]	Base de datos de carácter personal.	A	M	M
		Contabilidad del colegio	MA	M	A
	[classified]	Hoja de vida de los Estudiantes.	A	M	M
[D] datos / información	[Files]	Calificaciones	A	M	M
		Contabilidad	MA	M	A
		Archivos de actas	M	B	B
		Resoluciones (Actos administrativos y académicos)	M	B	B
		Observador del alumno	M	B	B
		Libro de Matricula	MA	B	M
	[backup]	Contabilidad institucional	A	M	M

	CÓDIGO DE ACTIVO	DESCRIPCIÓN	IMPACTO	PROBABILIDAD	RIESGO
		Documentos administrativos	A	B	M
[S] Servicios	[edi]	Diligenciamiento Matriz Chip	MA	B	M
[SW] Software - Aplicaciones informáticas	[os]	Sistema operativo Windows 7, Windows 8	M	M	M
	[sub]	Aplicación para el manejo de notas y reportes de los estudiantes.	M	M	M
	[dbms]	Base de datos para almacenar las notas de los estudiantes	A	M	M
	[office]	Office 2013, winrar, Adobe Acrobat Reader.	B	A	M
	[av]	Microsoft Security Essentials.	M	M	M
	[std]	Java, Cabri-Geom, Crocodile: Deep-Freze, Derive-Matem, Dev-C++ Portable, Gimp, WinCmapTools, MicromundosPro, Photoshop CS4 Portable_j89, TuxPaint, LEGO DIGITAL DESIGNER, Macromedia_Flash_8_(Portable), MECA NET, Microsoft Mathematics 4.0	M	A	M
[HW] Equipamiento informático (hardware)	[pc]	72 Equipos de escritorio salas de sistemas	B	M	B
		12 esquipos de escritorio aulas especializadas	B	M	B

	CÓDIGO DE ACTIVO	DESCRIPCIÓN	IMPACTO	PROBABILIDAD	RIESGO
		19 equipos de escritorio zona administrativa	B	M	B
	[mobile]	95 Portaltiles aulas especializadas	B	M	B
	[wap]	12 antenas de access point	M	M	M
	[switch]	4 switch 24 puertos	M	M	M
	[router]	Router CISCO 2900 Series.	M	M	M
	[print]	2 Impresoras salas de sistemas	B	MB	MB
		2 impresoras de multifunción (zona administrativa) 1 impresora chorro de tinta (zona administrativa) 1 impresora inalambrica (zona administrativa)	B	MB	MB
[COM] Redes de comunicaciones	[PSTN]	Acceso telefónico ETB	B	B	B
	[LAN]	Red Lan	MA	B	M
	[wifi]	Red Inalámbrica	MA	B	M
	[Internet]	ETB	M	B	B
[Media] Soportes de información	[cd]	Actas, resoluciones, observador de los estudiantes, agenda telefónicas, fotografías de los estudiantes por cursos, Soporte de contabilidad.	A	B	M
	[usb]	Copia de seguridad, documentos	A	B	M
	[dvd]	Proyecto educativo institucional, actas institucionales, documentos institucionales.	A	B	M

	CÓDIGO DE ACTIVO	DESCRIPCIÓN	IMPACTO	PROBABILIDAD	RIESGO
		Copia de Seguridad notas	A	B	M
	[printed]	Actas, resoluciones, observador del estudiantes, agenda telefónicas, fotografías de los estudiantes por cursos, Soporte de contabilidad, boletines, informes académicos, constancias, etc.	A	B	M
[AUX] Equipamiento auxiliar	[wire]	Instalaciones para el suministro de energía	M	B	B
	[furniture]	rack, armarios, archivadores, mesas, muebles, etc	B	B	B
[L] Instalaciones	[building]	Edificio sede colegio Luis Carlos Galán Sarmiento	MA	B	M
[P] Personal	[ue]	REDP	A	M	M
	[ui]	Administrativos, docentes	MA	A	MA
	[adm]	Docente de media Integrada e Informática	A	A	A
	[prov]	REDP, ETB	M	M	M

Fuente: Propiedad del autor

6. DEFINIR CUALES CONTROLES SON ACORDES PARA LA INSTITUCIÓN EDUCATIVA LUIS CARLOS GALÁN SARMIENTO, DE ACUERDO AL ANEXO A DE LA NORMA ISO 27001:2013

De acuerdo al análisis se definirá controles para neutralizar una amenaza a los activos encontrados en el Colegio Luis Carlos Galán Sarmiento. Estos controles se aplican para toda la institución educativa.

<table>
<tr><th>A.5</th><th colspan="3">POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN</th></tr>
<tr><td>A.5.1</td><td colspan="3">Orientación de la dirección para la gestión de la seguridad de la información.</td></tr>
<tr><td colspan="4">Objetivo: Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.</td></tr>
<tr><td>A.5.1.1</td><td>Políticas para la seguridad de la información</td><td colspan="2">Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Si aplica por que las políticas de seguridad son muy importantes para proteger los activos de toda la empresa.</td><td colspan="2">No cumple porque el Colegio Luis Carlos Galán Sarmiento no tiene un sistema de políticas de seguridad.</td></tr>
<tr><td>A.5.1.2</td><td>Revisión de la política de seguridad de la información</td><td colspan="2">Control: Las políticas para seguridad de la información se debe revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Si aplica por que las políticas de seguridad son muy importantes para proteger los activos de la empresa.</td><td colspan="2">No cumple porque el Colegio Luis Carlos Galán Sarmiento no tiene un sistema de políticas de seguridad.</td></tr>
</table>

A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
A.6.1	Organización Interna		
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del SGSI			
A.6.1.1	Seguridad de la Información Roles y Responsabilidades	**Control:** Se deben definir y asignar todas las responsabilidades de la seguridad de la información	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Si aplica porque en las políticas de seguridad los roles y responsabilidades son esenciales para el buen funcionamiento.		No cumple porque el Colegio Luis Carlos Galán Sarmiento no tiene un sistema de políticas de seguridad; por lo tanto no hay asignación de roles y responsabilidades.	
A.6.1.2	Separación de deberes	**Control:** Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Si aplica porque en las políticas de seguridad la organización disminuye el mal uso de los activos.		No cumple porque el Colegio Luis Carlos Galán Sarmiento no tiene un sistema de políticas de seguridad; por lo tanto no hay una separación de deberes para reducir las posibilidades de modificación no autorizada.	
A.6.1.3	Contacto con las autoridades.	**Control:** Se debe mantener contactos apropiados con las autoridades pertinentes.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
No aplica por que tiene éste servicio.		Si cumple porque el colegio tiene contacto con la autoridad.	
A.6.1.4	Contacto con grupos de interés especial	**Control:** Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Es importante que después de aplicada las políticas de seguridad, se mantenga el contacto con grupos de interés sobre seguridad.		Se cumple porque se tiene Interés sobre el bienestar del Carlos Galán Sarmiento.	

<table>
<tr><td>A.6</td><td colspan="2">ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>A.6.1</td><td colspan="2">Organización Interna</td></tr>
<tr><td>A.6.1.5</td><td>Seguridad de la información en Gestión de Proyectos</td><td>Control: La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto.</td></tr>
<tr><td colspan="2">APLICA</td><td>CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No es importante para las funciones del colegio Luis Carlos Galán Sarmiento</td><td colspan="2">No se maneja gestión de Proyectos</td></tr>
<tr><td>A.6.2</td><td colspan="2">Dispositivos Móviles y Teletrabajo</td></tr>
<tr><td colspan="3">Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles</td></tr>
<tr><td>A.6.2.1</td><td>Política para dispositivos móviles</td><td>Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles</td></tr>
<tr><td colspan="2">APLICA</td><td>CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Es importante para mantener el buen funcionamiento de la institución.</td><td colspan="2">No hay políticas de seguridad para dispositivos móviles.</td></tr>
<tr><td>A.6.2.2</td><td>Teletrabajo</td><td>Control: Se deben implementar una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo</td></tr>
<tr><td colspan="2">APLICA</td><td>CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No aplica porque no política de la secretaria de educación. No se fomenta Teletrabajo en la institución.</td><td colspan="2">No cumple porque no está dentro de lo académico.</td></tr>
</table>

A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	
A.7.1	Antes de asumir el empleo	
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran		
A.7.1.1	Selección	**Control:** Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
No aplica porque el personal administrativo, docente y vigilancia lo contrata directamente la secretaria de educación.		No cumple por que la institución no contrata directamente al personal.
A.7.1.2	Términos y condiciones del empleo	**Control:** Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
El factor más importante en la seguridad es el usuario; por eso sería enriquecedor las indicaciones aconsejable para el caso.		El personal de trabajo mantiene el respeto por los activos de la empresa.
A.7.2	Durante la ejecución del empleo	
Objetivo: Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad dela información y las cumplan		
A.7.2.1	Responsabilidades de la Dirección	**Control:** La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Es el importante que todos los empleados y población Galanista tengan claros los acuerdos con las		No se hace el proceso a los empleados sobre información de seguridad porque no hay.

políticas y procedimiento pactados en la organización.		
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**	
A.7.1	Antes de asumir el empleo	
A.7.2.2	Toma de conciencia, educación y formación de la Seguridad de la Información	**Control:** Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Capacitación para que el personal administrativo y los docentes a cargo estén actualizado sobre seguridad informática.		No se presenta ésta situación en la institución.
A.7.2.3	Proceso disciplinario	**Control:** Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Se aplica para tener mejor control en la seguridad.		Si presenta ésta situación la institución.
A.7.3	Terminación y cambio de empleo.	
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.		
A.7.3.1	Terminación o cambio de responsabilidades de empleo	**Control:** Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Este proceso es ajeno a la institución		No se hace el proceso a los empleados.

<table>
<tr><td>A.8</td><td colspan="3">GESTIÓN DE ACTIVOS</td></tr>
<tr><td>A.8.1</td><td colspan="3">Responsabilidad por los activos</td></tr>
<tr><td colspan="4">Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.</td></tr>
<tr><td>A.8.1.1</td><td>Inventario de Activos</td><td colspan="2">Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activo</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Es importante la identificación de archivos para conservar el buen uso de los mismos.</td><td colspan="2">La almacenista realiza el respectivo inventario de acuerdo con la información e instalación de procedimientos establecidos.</td></tr>
<tr><td>A.8.1.2</td><td>Propiedad de los activos</td><td colspan="2">Control: Los activos mantenidos en el inventario deben ser propios.</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Si aplica porque cada dependencia debe tener sus propios activos.</td><td colspan="2">Los activos son propios.</td></tr>
<tr><td>A.8.1.3</td><td>Uso Aceptable de los Activos</td><td colspan="2">Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Es importante informar a los usuarios sobre los procedimientos de la información.</td><td colspan="2">hay reglas implementadas para socializar</td></tr>
<tr><td>A.8.1.4</td><td>Devolución de Activos</td><td colspan="2">Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Si aplica porque el Colegio Luis Carlos Galán sarmiento exige a los docentes estar a paz y salvo con los activos correspondiente a almacén y Biblioteca.</td><td colspan="2">A final de año o finalización de contratos de docentes provisional; el almacenista genera un formulario por cada docente para la verificación de los activos de la sala de sistemas y biblioteca y así se cierra el inventario anual.</td></tr>
</table>

A.8	**GESTIÓN DE ACTIVOS**			
A.8.2	Clasificación de la información.			
Objetivo: Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización				
A.8.2.1	Clasificación de la Información	**Control:** La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o modificación no autorizada		
APLICA		**CUMPLE**		
SI	**NO**	**SI**	**NO**	
Aplica porque se tiene que clasificar la información en: secreta, confidencial, pública o reservada.		La información no se encuentra clasificada, según el criterio de la clasificación de la información.		
A.8.2.2	Etiquetado de la Información	**Control:** Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.		
APLICA		**CUMPLE**		
SI	**NO**	**SI**	**NO**	
El Colegio Luis Carlos Galán Sarmiento debe contar con el proceso de etiquetado de información para su respectiva clasificación		Actualmente el personal administrativo lleva un esquema de etiquetado de información de forma básica.		
A.8.2.3	Manejo de Activos	**Control:** Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización		
APLICA		**CUMPLE**		
SI	**NO**	**SI**	**NO**	
No aplica porque ya se está llevando los procedimientos para el manejo de los activos.		Los manejos de activos que se llevan en el Colegio Luis Carlos Galan Sarmiento son llevados por la señora almacenista, cumpliendo con la clasificación.		
A.8.3	Manejo de medios de soporte.			
Objetivo: Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.				
A.8.3.1	Gestión de medios de Soporte Removibles	**Control:** Se deben implementar procedimientos para la gestión de		

		medios de soporte removibles, de acuerdo con el esquema de clasificación adoptado por la organización
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
Tener presente las políticas de seguridad para realizar gestión de medios de soporte removible.		Tiene las reglas para el manejo de soporte removible.	
A.8.3.2	Disposición de los medios de soporte	**Control:** Se debe disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
No aplica porque los documentos están en buen cuidado.		Se guarda en un archivador de manera seguro donde reposa todo el historial del colegio.	
A.8.3.3	Transferencia de medios de soporte físicos	**Control:** Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
No aplica pues, las seguridad a la informaciòn en la transferencia de medios se esta cumpliendo.		Si cumple porque se hace todas las medidas de seguridad para que el paquete llegue a su destino sin problema alguno.	

A.9	**CONTROL DE ACCESO**	
A.9.1	**Requisitos del Negocio para el Control de Acceso**	
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información		
A.9.1.1	Política de control de acceso	**Control:** Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
Si aplica porque es necesario el control de acceso para el colegio Luís Calos Galán.		No cumple porque en el colegio no hay políticas de control de acceso.	
A.9.1.2	Acceso a redes y a servicios en red	**Control:** Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	
APLICA		**CUMPLE**	

SI	NO	SI	NO
Es necesario implementar las políticas de seguridad para proteger los activos que son vulnerables.		La red tiene acceso público.	

A.9.2	GESTIÓN DE ACCESO DE USUARIOS
Objetivo: Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios	

A.9.2.1	Registro y cancelación del registro de usuarios	**Control:** Se debe implementar un proceso formal de registro y de cancelación del registro para posibilitar la asignación de los derechos de acceso.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Si aplica porque es necesario que el personal administrativo y toda la institución generen éste tipo de seguridad para todos los usuarios.		No se cumple por que no estas las políticas para el acceso de registro de usuarios.	
A.9.2.2	Suministro de acceso de usuarios	**Control:** Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
No aplica porque ya hay una entidad que cubre esa necesidad.		No aplica ya que Redp se encarga de dicha labor.	
A.9.2.3	Gestión de derechos de acceso privilegiado	**Control:** Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Si aplica porque es necesario que el colegio implante este acceso de privilegios.		No cumple porque el colegio no ha implementado esta política a los usuarios.	
A.9.2.4	Gestión de información de autenticación secreta de usuarios.	**Control:** La asignación de información de autenticación secreta se debe controlar por medio de un procedimiento de gestión formal.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
No aplica pues hay una entidad encargada de la asignación de información de autenticación.		No cumple porque no se realiza gestión de información de autenticación secreta de usuarios en la institución	

A.9.2.5	Revisión de los derechos de acceso de usuarios	**Control:** Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Si aplica porque es vital que el colegio Luis Carlos Sarmiento haga revisión de los derechos de acceso de usuarios para proteger los activos.		No aplica porque el correo no hace revisión de los derechos de acceso de usuarios.
A.9.2.6	Cancelación o ajuste de los derechos de acceso	**Control:** Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procedimiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Si aplica porque es importante dejar claro para la institución los derechos de acceso.		No cumple porque el Colegio no lo tiene implementado el ajuste de los derechos de acceso.
A.9.3	**Responsabilidades de los usuarios**	
Objetivo: Hacer que los usuarios rindan cuentas por la custodia de su información de autenticación		
A.9.3.1	Uso de información secreta	**Control:** Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Aplica por lo relevante que tiene la información para la institución.		No cumple porque no hay uso de información secreta
A.9.4	**Control de Acceso a Sistemas y Aplicaciones**	
Objetivo: Prevenir el uso no autorizado de sistemas y aplicaciones.		
A.9.4.1	Restricción del acceso a la información	**Control:** El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**

Si aplica porque es necesario que el colegio realice las restricciones de acceso a la información.		No cumple porque no se tiene establecidas el acceso a la información.
A.9.4.2	Procedimiento de Conexión Segura	**Control:** Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
No aplica porque no se hace conexión remota.		No cumple porque no hay conexión remota.
A.9.4.3	Sistema de gestión de contraseñas	**Control:** Los sistemas de gestión de contraseñas deben ser interactivos y deberían asegurar la calidad de las contraseñas
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
Si aplica ya que es necesario para el control de gestión de contraseña y mantener seguridad al colegio.		No hay una conexión remota.
A.9.4.4	Uso de programas utilitarios privilegiados	**Control:** Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
Si aplica porque es necesario para la seguridad el de hacer uso privilegiados ya que se hace más control.		La entidad encargada tiene restringido algún acceso al sistema, pero el colegio no tiene políticas para controles de las aplicaciones.
A.9.4.5	Control de Acceso a Códigos Fuente de Programas.	**Control:** Se debe restringir el acceso a códigos fuente de programas.
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
No aplica por que el nivel de conocimiento de manipulación de código fuente de programa es básico.		No cumple por que el nivel de escolaridad es académico, sin tener la preparación para manipular código fuente.

A.10	CRIPTOGRAFIA		
A.10.1	**Controles Criptográficos**		
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.			
A.10.1.1	Política sobre el uso de controles Criptográficos.	**Control:** Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para protección de información.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
El Colegio no ha visto la necesidad de implantarlo.		El Colegio Luis Carlos Galán Sarmiento no hace uso de técnicas criptográfica.	
A.10.1.2	Gestión de Claves.	**Control:** Se debe desarrollar e implementar una política el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Con el flujo de información que se maneja en el colegio, no se ve la necesidad del uso de técnicas criptográficas.		Como el colegio no utiliza criptografía, entonces no hay tiempo de vida de claves criptográficas para aplicar.	

A.11	SEGURIDAD FÍSICA Y AMBIENTAL		
A.11.1	**Áreas Seguras**		
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización			
A.11.1.1	Perímetro de Seguridad Física.	**Control:** Se debe definir y usar perímetros de seguridad, y usuarios para proteger áreas que contenga información confidencial o critica, e instalaciones de manejo de información-	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Cumple con requisitos de seguridad que recomienda la ley.		Tiene normas de seguridad	
A.11.1.2	Controles físico de entrada.	**Control:** Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	
APLICA		**CUMPLE**	

SI	NO	SI	NO
Al tener control a los accesos restringido no se ve la necesidad de reforzarlo o cambiarlo.		Se tiene control a los sitios de acceso restringido por agentes de seguridad o docente encargado.	
A.11.1.3	Seguridad de oficinas, salones e instalaciones.	**Control:** Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Ya tiene seguridad física a oficinas, salones e instalaciones.		El colegio cuenta con control de vigilancia a todos los salones y oficinas administrativas.	
A.11.1.4	Protección contra amenazas externas y ambientales	**Control:** Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Cuenta con la protección de amenazas		Cumple con protección física contra desastres naturales y demás.	
A.11.1.5	Trabajo en áreas seguras	**Control:** Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Esta establecido los procedimientos y restricciones al área de sistemas o áreas seguras.		Se aplica pues, los espacios dados para áreas de sistemas solo son permitido para el personal autorizado.	
A.11.1.6	Área de despacho y carga.	**Control:** Se debe controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Se cumple que el lugar donde llega personal no autorizado se encuentra aislado.		La orientadora encargada de recibir los refrigerios y de despachar los mismos se encuentra en un lugar aislado de procesamiento de información.	
A.11.2	**Equipos.**		
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.			
A.11.2.1	Ubicación y protección de los equipos.	**Control:** Los equipos se deben estar ubicados y protegidos para reducir los	

		riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado.
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
No aplica pues, los equipos están en una sala, protegida de riesgos naturales. Para el acceso a ellos hay que desactivar las alarmas en portería; donde exclusivamente tienen la clave 3 profesores del área de sistemas.		Las áreas de sistemas están protegidas de peligros físicos y ambientales que puedan ocasionarles daño a los equipos y a la institución.	
A.11.2.2	Servicios Públicos de soporte	**Control:** Los equipos se deben proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte**.**
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
Cumple con la protección de las fallas.		Cuenta con estabilizadores. Cuando hay tormentas eléctricas, se recomienda apagar los equipos.	
A.11.2.3	Seguridad del cableado	**Control:** El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptaciones, interferencia o daño.
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
No aplica porque el cableado estructurado está en canaletas.		Está protegido por canaletas estandarizadas.	
A.11.2.4	Mantenimiento de equipos	**Control:** Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
No aplica por que la información está disponible e integra.		La información está disponible cuando se necesita.	
A.11.2.5	Retiro de activos	**Control:** Los equipos, información software no se deben retirar de su sitio sin autorización previa.
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
Es importante generar políticas sobre los activos del colegio y de las responsabilidades que deben tener con ellos.		Ninguno del colegio está autorizado para retirar activos.	

A.11.2.6	Seguridad de equipos y activos fuera del predio.	**Control:**. Se debe aplicar medidas de seguridad a los activos que se encuentra fuera de los predios de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichos predios.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
No aplica porque esta reglamentación está en el almacén.		No cumple porque esta los procedimientos de llevan a cabo.
A.11.2.7	Disposición segura o reutilización de equipos.	**Control:** Se debe verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobre escrito en forma segura antes de su disposición o reuso.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
No aplica porque Redp es el responsable de valorar los equipos que contengan medios de almacenamiento.		Redp es el encargado de hacer esta verificación.
A.11.2.8	Equipos sin supervisión de los usuarios.	**Control:** Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
No aplica ya que todos los equipos de cómputo se encuentran con supervisión.		Los equipos que existen en la institución tienen su respectiva asignación; por lo tanto no hay sobrantes que queden sin supervisión.
A.11.2.9	Política de escritorio limpio y pantalla limpia.	**Control:** Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Si aplica porque es importante dejar escrito y plasmado las políticas de escritorio limpio para evitar dejar documentos innecesarios.		Existe Software o congelador FREE para bajar el almacenamiento en la partición C:

<table>
<tr><td>A.12</td><td colspan="3">SEGURIDAD DE LAS OPERACIONES</td></tr>
<tr><td>A.12.1</td><td colspan="3">Procedimientos operacionales y responsabilidades.</td></tr>
<tr><td colspan="4">Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.</td></tr>
<tr><td>A.12.1.1</td><td>Procedimientos de operación documentales.</td><td colspan="2">Control:. Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Todos los documentos se encuentran disponibles a los usuarios que lo necesiten y que tenga autorización de utilizarla.</td><td colspan="2">Al solicitar el historial académico de los estudiantes se encuentra disponible.</td></tr>
<tr><td>A.12.1.2</td><td>Gestión de Cambios</td><td colspan="2">Control:. Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.</td></tr>
<tr><td colspan="2">AP LICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No aplica porque no se encuentra una política establecida en la institución.</td><td colspan="2">No cumple porque las políticas no existen</td></tr>
<tr><td>A.12.1.3</td><td>Gestión de Capacidad</td><td colspan="2">Control:. Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Redp es el encargado de estudio y proyecciones a futuras sobre el área de sistemas.</td><td colspan="2">Redp realiza la planeación de ajustes, proyecciones, para asegurar el desempeño requerido del sistema.</td></tr>
<tr><td>A.12.1.4</td><td>Separación de los ambientes de desarrollo, ensayo y operación</td><td colspan="2">Control:. Se deben separar los ambientes de desarrollo, ensayo y operativos, para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional.</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No aplica por que los espacios están asignados para la labor establecida por la institución.</td><td colspan="2">Cada espacio es asignado para cada labor.</td></tr>
</table>

<table>
<tr><td>A.12.2</td><td colspan="3">Protección contra Códigos Maliciosos</td></tr>
<tr><td colspan="4">Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos</td></tr>
<tr><td>A.12.2.1</td><td colspan="2">Controles contra códigos maliciosos</td><td>Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Es necesario dar conciencia a docentes y personal administrativo para proteger el sistema de códigos maliciosos.</td><td colspan="2">No hay conciencia en códigos maliciosos.</td></tr>
<tr><td>A.12.3.1</td><td colspan="2">Copias de respaldo de la información</td><td>Control: Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Si aplica porque es importante que el colegio haga normas de copia de respaldo de la información para asegurar sus activos.</td><td colspan="2">No cumple porque no se encuentra establecida una política de seguridad sobre copias de respaldo de información.</td></tr>
<tr><td>A.12.4</td><td colspan="3">Registro y seguimiento</td></tr>
<tr><td colspan="4">Objetivo: Registrar eventos y generar evidencia</td></tr>
<tr><td>A.12.4.1</td><td colspan="2">Registro de eventos</td><td>Control: Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepcionales, fallas y eventos de seguridad de la información.</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Si aplica porque es necesario implementar las políticas del reporte de actividades y fallos de la seguridad.</td><td colspan="2">No cumple porque no hay establecida políticas en el colegio sobre registro de eventos.</td></tr>
<tr><td>A.12.4.2</td><td colspan="2">Protección de la información de registro</td><td>Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
</table>

SI	NO	SI	NO
No aplica porque la protección de la información de registro no esta implementado en el colegio.		No cumple porque la protección de la información de registro no esta en el colegio	
A.12.4.3	Registros del administrador y del operador.	**Control:** Las actividades del administrador y del operador del sistema se deben registrar y los registros se deben proteger y revisar con regularidad.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Si aplica porque es importante que la institución registre las actividades que realiza el administrador con respecto a la seguridad y a la operación del sistema.		No cumple porque el colegio no realiza un seguimiento a los administradores o operador de Redp que ingresa, sobre las funciones que realiza.	
A.12.5	Control de Software Operacional.		
Objetivo: Asegurarse de la integridad de los sistemas operacionales.			
A.12.5.1	Instalación de software en sistemas operativos	**Control:** Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
No aplica porque el colegio no se encarga de tal procedimiento.		El agente encargado de instalación de software realiza los procedimientos.	
A.12.6	Gestión de vulnerabilidad técnica.		
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas			
A.12.6.1	Gestión de las vulnerabilidades técnicas	**Control:** Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
No aplica porque la institución no cuenta con sistema de información propios, estos sistemas de información son suministrados por la secretaria y ministerio de educación.		No cumple porque no hay aplicativo para la gestión de las vulnerabilidades técnicas.	

A.12.6.2	Restricciones sobre la instalación de software	**Control:** Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
Si aplica porque son políticas necesarias para implantar condiciones a los usuarios.		El personal encargado realiza los procedimientos para la instalación de software.	
A.12.7	Consideraciones sobre auditorías de sistemas de información.		
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.			
A.12.7.1	Controles sobre auditorías de Sistemas de Información	**Control:** Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
No aplica porque el colegio no se encarga directamente de realizar la auditora de sistemas de información.		La secretaria de educación se encarga de estos procesos.	

A.13	**SEGURIDAD DE LAS COMUNICACIONES**	
A.13.1	**Gestión de la Seguridad de las Redes.**	
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte. .		
A.13.1.1	Controles de redes	**Control:** Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
No aplica porque el colegio no se encarga directamente de realizar la auditora de sistemas de información.		La secretaria de educación se encarga de estos procesos.	
A.13.1.2	Seguridad de los servicios de red.	**Control:** Se deben identificar los mecanismos de seguridad y los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten

		internamente o se contraten externamente.
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
No aplica porque el colegio Luis Carlos Galán Sarmiento no realiza dicho procedimiento de mecanismo de seguridad.		La entidad encargada realiza los protocolos de seguridad.	
A.13.2	Transferencia de información		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa			
A.13.2.1	Políticas y procedimientos de transferencia de información	**Control:** Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información, mediante el uso de todo tipo de instalaciones de comunicaciones.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
No aplica por que los controles de transferencias para proteger la información se está aplicando a cada envio de información.		Si cumple porque se lleva a cabo los controles de transferencia de archivos.	
A.13.2.2	Acuerdos sobre transferencia de información.	**Control:** Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Se debe tener políticas en el colegio que tenga establecidos los acuerdos sobre transferencia de información.		No hay políticas establecidas para los acuerdos de transferencia de información	
A.13.2.3	Mensajes electrónicos	**Control:** Se debe proteger apropiadamente la información incluida en los mensajes electrónicos.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
El colegio mantiene una comunicación.		El colegio tiene un correo institucional que sirve como correspondencia interna y externa, además tiene correspondencia física tanto externa como interna.	
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	**Control:** Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que	

		reflejen las necesidades de la organización para la protección de la información.
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
No aplica poque lo realiza directamente la secretaria de educaciòn		No cumple po que lo hace directamente la secretaria de educaciòn	

A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**	
A.14.1	Requisitos de seguridad de los sistemas de información	
Objetivo: Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas.		
A.14.1.1	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información	**Control:** Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
No aplica porque los activos que están ingresando al colegio están adquiriendo las mismas condiciones de segurid ad que los existentes.		Los activos que ingresen automáticamente tienen las mismas condiciones que sus similares.	
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	**Control:** La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
No aplica, porque es controlado por la secretaria de educaciòn		Si cumple porque se realiza el control asignado.	
A.14.1.3	Protección de transacciones de	**Control:** La información involucrada en las transacciones de servicios de aplicaciones se debe proteger para

	servicios de aplicaciones.	prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes. La divulgación no autorizada y la duplicación o reproducción de mensajes no autorizados.
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
No aplica porque estas transacciones incompletas no han tenido el colegio.		No cumple porque el colegio no posee la aplicación de servicios de aplicaciones.	
A.14.2	Seguridad en los procesos de desarrollo y de soporte		
Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.			
A.14.2.1	Política de desarrollo seguro	**Control:** Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas a los desarrollos dentro de la organización.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
No aplica porque la actividad de desarrollo de software no está en la institución.		No aplica porque no hay desarrollo de software dentro de la institución.	
A.14.2.2	Procedimiento de control de cambios en sistemas	**Control:** Los cambios a los sistemas dentro del ciclo de vida de desarrollo de software y de sistemas a los desarrollos dentro de la organización.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
No aplica porque la entidad encargada del mantenimiento de los sistemas en el colegio realiza dicha labor.		No cumple porque esos cambios que se presentan lo atiende Redp	
A.14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones.	**Control:** Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y poner a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad organizacionales.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
No aplica porque el colegio no realiza este tipo de procedimiento		No aplica al colegio por que los encargados de la plataforma es directamente la secretaria de Educación.	

A.14.2.4	Restricciones sobre los cambios de paquetes de software	**Control:** Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
No aplica porque el colegio esta fuera de estas labores de sistemas.		No cumple en el colegio porque èste control no hace parte de las labores del colegio.
A.14.2.5	Principios de construcción de sistemas de seguros	**Control:** Se deben establecer, documentar y mantener principios para la organización de sistemas seguros, y aplicarlos a cualquier trabajo de implementación de sistemas de información.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
No aplica porque no es función del Colegio Luis Carlos Galán Sarmiento.		Estrictamente la labor lo hace externamente.
A.14.2.6	Ambiente de desarrollo seguro.	**Control:** Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
No aplica porque se está llevando a cabo junto al área encargada de sistemas.		El colegio junto a Redp se encarga de proteger físicamente y a nivel de software de todos los activos de la institución.
A.14.2.7	Desarrollo contratado externamente	**Control:** La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas subcontratados.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
No aplica porque la institución lleva los requerimientos necesarios para los subcontratados.		El colegio hace los requerimientos para la aceptación y el buen uso de los activos de la institución.
A.14.2.8	Pruebas de seguridad de sistemas	**Control:** Durante el desarrollo se deben llevar a cabo ensayos de funcionalidad de la seguridad.

APLICA		CUMPLE	
SI	**NO**	**SI**	**NO**
No aplica porque la entidad encargada lo esta realizando.		La empresa encargada del mantenimiento de los sistemas cumple con estas políticas.	
A.14.2.9	Pruebas de aceptación de sistemas	**Control:** Para los sistemas de información nuevos, actualizaciones y nuevas versiones se deben establecer programas de ensayo y criterios relacionados.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
No aplica porque el colegio no se encarga de este control de actualizaciones y nuevas versiones.		La empresa cumple con todas estos controles.	

A.14.3	Datos de ensayo	
Objetivo: Asegurar la protección de los datos usados para ensayos.		
A.14.3.1	Protección de datos de ensayo	**Control:** Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
No aplica porque el colegio lleva èste control		Los funcionarios externos e internos protegen y controlan los activos del Colegio.	

A.15	**RELACIONES CON LOS PROVEEDORES**	
A.15.1	Seguridad de la Información en las Relaciones con los Proveedores	
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores		
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	**Control:** Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
No aplica porque tiene la documentación necesaria para el		El colegio lleva registros de información de proveedores y condiciones de trabajo.	

<table>
<tr><td colspan="2">proceso de visita de proveedores a la institución.</td><td></td></tr>
<tr><td>A.15.1.2</td><td>Tratamiento de la seguridad dentro de los acuerdos con proveedores</td><td>Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puedan tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.</td></tr>
<tr><td colspan="2">APLICA</td><td>CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Si aplica porque se desea implementar políticas para el tratamiento de la seguridad en los proveedores.</td><td>No cumple porque no tiene políticas de seguridad.</td></tr>
<tr><td>A.15.1.3</td><td>Cadena de suministro de tecnología de información y comunicación.</td><td>Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.</td></tr>
<tr><td colspan="2">APLICA</td><td>CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">El colegio Luis Carlos Galán Sarmiento debe gestionar las políticas en el colegio sobre la tecnología de información y comunicación.</td><td>La secretaria de educación se encarga de los acuerdos con los proveedores.</td></tr>
<tr><td>A.15.2</td><td colspan="2">Gestión de la prestación de servicios de proveedores</td></tr>
<tr><td colspan="3">Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.</td></tr>
<tr><td>A.15.2.1</td><td>Seguimiento y revisión de los servicios de los proveedores</td><td>Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.</td></tr>
<tr><td colspan="2">APLICA</td><td>CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Se realiza el proceso de seguimiento a proveedores que visitan la institución.</td><td>El colegio lleva un registro con todos los proveedores y sus funciones.</td></tr>
<tr><td>A.15.2.2</td><td>Gestión de cambios a los servicios de los proveedores</td><td>Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes,</td></tr>
</table>

		teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
No aplica porque el colegio no se ocupa de dicha labor.		El colegio da un reporte del servicio del proveedor pero la secretaria de educación es la que gestiona cambios de servicios.	

A.16	**GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN**	
A.16.1	**Gestión de los Incidentes y las Mejoras en la Seguridad de la Información**	
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidad.		
A.16.1.1	Responsabilidades y procedimientos	**Control:** Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Si aplica porque se debe contar con los procedimientos de responsabilidades y procedimientos.		No cuple porque no tiene procedimientos establecidos.	
A.16.1.2	Informe de eventos de seguridad de la información	**Control:** Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Si aplica porque es necesario tener esta política implementada en el colegio.		No cumple porqueno se cuenta con este procedimiento.	
A.16.1.3	Informe de debilidades de seguridad de la información.	**Control:** Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios

APLICA		CUMPLE	
SI	**NO**	**SI**	**NO**
Si aplica porque es necesario contar con el personal idóneo para dicho trabajo.		No cumple porque no se cuenta con ésta política de informe de debilidades de seguridad de la información.	
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	**Control:** Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
No aplica porque el colegio no hace este tipo de evento.		El colegio no hace este tipo de control de eventos de seguridad.	
A.16.1.5	Respuesta a incidentes de seguridad de la información.	**Control:** Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Si se aplica porque es necesario la implementación de incidentes de seguridad de la información de acuerdo a procedimientos.		No cumple porque no se cuenta con dicha seguridad	
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	**Control:** El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Si aplica porque es necesario tener el registro de la trazabilidad de los incidentes de seguridad.		No cumple porque no tiene la trazabilidad de los incidentes de seguridad.	
A.16.1.7	Recolección de evidencia	**Control:** La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Si aplica porque es necesaria registrar la recolección de evidencia.		El colegio no hace este tipo de control de eventos de seguridad.	

<table>
<tr><td>A.17</td><td colspan="3">ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO</td></tr>
<tr><td>A.17.1</td><td colspan="3">Continuidad de Seguridad de la Información</td></tr>
<tr><td colspan="4">Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.</td></tr>
<tr><td>A.17.1.1</td><td>Planificación de la continuidad de la seguridad de la información.</td><td colspan="2">Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres.</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No aplica porque la secretaria se encarga directamente de dicha función.</td><td colspan="2">La secretaria de educación tiene controles establecidos.</td></tr>
<tr><td>A.17.1.2</td><td>Implementación de la continuidad de la seguridad de la información</td><td colspan="2">Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Se ejecuta el proceso de control por la secretaria de educación.</td><td colspan="2">Cumple con ciertas normas, procesos y controles en seguridad de la información. La secretaria de educación es la encargada de dicho proceso</td></tr>
<tr><td>A.17.1.3</td><td>Verificación, revisión y evaluación de la continuidad de la seguridad de la información.</td><td colspan="2">Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que los válidos y eficaces durante situaciones adversas.</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No aplica porque el colegio no hace este tipo de evento.</td><td colspan="2">El colegio no hace este tipo de control de verificación y revisión de evaluación.</td></tr>
<tr><td>A.17.2</td><td colspan="3">Redundancia</td></tr>
<tr><td colspan="4">Objetivo: Asegurarse de la disponibilidad de instalaciones de procesamiento de información.</td></tr>
<tr><td>A.17.2.1</td><td>Disponibilidad de instalaciones de</td><td colspan="2">Controles: Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente</td></tr>
</table>

	procesamiento de información.	para cumplir los requisitos de disponibilidad	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
No aplica la información es suministrada a la secretaria de educación.		Si cumple porque la secretaria tiene establecido la parte contable y académica.	

A18	**CUMPLIMIENTO**	
A.18.1	**Cumplimiento de los Requisitos Legales y Contractuales**	
Objetivo: Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.		
A.18.1.1	Identificación de los requisitos de legislación y contractuales aplicables	**Controles:** Se deben identificar, documentar y mantener actualizados explícitamente todos los requisitos legislativos estatutarios, de reglamentación y contractuales pertinentes, y el enfoque de la organización para cada sistema de información y para la organización.
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
No aplica porque el colegio no hace este tipo de control		El colegio no hace este tipo de control.	
A.18.1.2	Derechos de Propiedad Intelectual	**Controles:** Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados.
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
No se aplica porque es política nacional.		Si se cumple implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos.	
A.18.1.3	Protección de registros	**Control:** Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
APLICA		**CUMPLE**

SI	**NO**	**SI**	**NO**
Descripción: Hay control para la protección de registros contra perdidas, destrucción, falsificación y acceso no autorizado.		Descripción: Hay control para la protección de registros contra perdidas, destrucción, falsificación y acceso no autorizado.	
A.18.1.4	Privacidad y protección de datos personales	**Control:** Se deben asegurar la privacidad y la protección de la información identificable personalmente, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable**.**	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Si aplica porque es necesario implementar la política de privacidad y protección.		No cumple porque no está implementado dicha política.	
A.18.1.5	Reglamentación de Controles Criptográficos.	**Controles:** Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
El Colegio no ha visto la necesidad de implantarlo.		El Colegio Luis Carlos Galán Sarmiento no hace uso de técnicas criptográfica.	
A.18.2	Revisiones de seguridad de la información		
A.18.2.1	Revisión independiente de la seguridad de la información.	**Control:** El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, la políticas, los procesos y los procedimientos para seguridad de la información se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
No aplica porque en el colegio se lleva a cabo dicho control		Si cumple en la gestión de la seguridad de la información.	
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	**Control:** Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	
APLICA		**CUMPLE**	

SI	NO	SI	NO
Descripción: Realizar el cumplimiento con las políticas y normas de seguridad.		Descripción: No hay política de seguridad	
A.18.2.3	Revisión del cumplimiento técnico	**Control:** Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Descripción: No hay políticas ni normas de seguridad.		Descripción: No hay política de seguridad en el colegio Luis Carlos Galán Sarmiento.	

Fuente: Propiedad de los autores

7. PROPONER POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA INSTITUCIÓN EDUCATIVA LUIS CARLOS GALÁN SARMIENTO TENIENDO EN CUENTA LOS CONTROLES APLICADOS DE LA NORMA ISO 27001:2013

7.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

7.1.1 Políticas generales de la seguridad informática

Las Políticas de Seguridad de la Información, surgen como una herramienta institucional para concienciar a cada uno de los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la empresa sobre la importancia y sensibilidad de la información y servicios críticos, de tal forma que le permitan desarrollar adecuadamente sus labores y cumplir con su propósito misional.

Objetivo

Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes

Aplicabilidad

Estas son políticas que aplican a la rectoría, coordinadora, Jefes de área, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de la organización.

Directrices

- ✓ Mantener un inventario actualizado de sus activos de información, bajo la responsabilidad de cada propietario de información y centralizado por el Área Información y Sistemas.
- ✓ Verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.

7.1.2 Revisión de la política de seguridad de la información

La política de seguridad de la información se debe revisar en fechas estipuladas para generar el buen flujo de la información.

Aplicabilidad

Estas son políticas que aplican a la rectoría, coordinadora, Jefes de área, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de la organización.

Directrices

- ✓ Cada semana se debe realizar Backup a los activos importantes de la institución.
- ✓ Todos los documentos de la institución deben ser enviados por un correo institucional.
- ✓ El colegio debe tener un dominio propio para su uso personal.
- ✓ Todos los docentes y personal administrativo deben respetar las fechas de revisión de la política de seguridad de la información.
- ✓ Todos los miembros de la comunidad educativa deben hacerse participes de los resultados de la revisión de la política de seguridad.

7.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

7.2.1 Seguridad de la Información Roles y Responsabilidades

La seguridad de la información hace un análisis del proceso de responsabilidad y autoridad en la seguridad de los activos de la información. Se deben definir y asignar todas las responsabilidades de la seguridad de la información.

Objetivo

Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del SGSI.

Aplicabilidad

Estas son políticas que aplican a la rectoría, coordinadora, Jefes de área, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de la organización.

Directrices

- ✓ Cada funcionario debe ser responsable de su rol asignado.
- ✓ El personal administrativo o docente no puede asignar roles a sus compañeros de trabajo.
- ✓ El funcionario debe respetar las pautas implantadas por el administrador de sistemas.

7.3 DISPOSITIVOS MÓVILES Y TELETRABAJO

7.3.1 Política para dispositivos móviles

Utilizar los dispositivos móviles en las diferentes ramas del conocimiento con las precauciones del manejo a nivel de hardware y software.

Objetivo

Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

Aplicabilidad

Estas son políticas que aplican para Docentes y estudiantes.

Directrices

- ✓ Es estudiantes no pueden ingresar a redes sociales.
- ✓ Los estudiantes no pueden instalar software en los dispositivos móviles.
- ✓ Los estudiantes deben tener únicamente el acceso a los dispositivos móviles para consultas académicas.
- ✓ Los estudiantes al finalizar la clase deben apagar el dispositivo móvil.

7.4 DURANTE LA EJECUCIÓN DEL EMPLEO

7.4.1 Responsabilidades de la Dirección

Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.

Objetivo

Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

Aplicabilidad

Estas son políticas que aplican al personal administrativo de la institución.

Directrices

- ✓ No deben tener acceso a los sistemas, personas ajenas a la institución.
- ✓ Se debe quitar vínculos con personas que ya no hagan parte de la institución.
- ✓ No permitir que docentes, alumnos y personal administrativo se pueda conectar a internet con el servicio del colegio.
- ✓ No conectar usb, cargadores, celulares u otros dispositivos ajenos a la institución.

7.4.2 Toma de conciencia, educación y formación de la Seguridad de la Información

Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.

Objetivo

Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad dela información y las cumplan.

Aplicabilidad

Estas son políticas que aplican a la rectoría, coordinadora, Jefes de área, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de la organización

Directrices

- ✓ Los computadores deben estar restringidos de páginas no autorizadas.
- ✓ A los estudiantes les queda rotundamente sacar los computadores del área asignada.
- ✓ Los contratistas que ingresen al colegio deben presentar su cedula y dejar un carnet de identificación.

7.5 CONTROL DE ACCESO

7.5.1 Acceso a redes y a servicios en red

Objetivo

Limitar el acceso a información y a instalaciones de procesamiento de información

Aplicabilidad

Estas son políticas que aplican a la rectoría, coordinadora, Jefes de área, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de la organización.

Directrices

- ✓ El personal administrativo no compartirá archivos visibles en la red.
- ✓ Está prohibido que Redp suministre clave de acceso Wifi a los docentes, personal administrativo y a los estudiantes.

7.5.2 Restricción del acceso a la información

Directrices

- ✓ Está prohibido que Redp entregue la clave de acceso por administración a los docentes y a toda la comunidad educativa.
- ✓ Redp debe colocarle contraseña al Setup para que no cambien la configuración de la Board.

7.6 SEGURIDAD DE LAS OPERACIONES

7.6.1 Controles contra códigos maliciosos

Directrices

- ✓ No abrir correos de procedencia desconocida.
- ✓ Nadie de la institución está autorizado para descargar programas.
- ✓ Verificar que las páginas web donde se ingresa sean seguras.

7.7 REGISTRO Y SEGUIMIENTO

7.7.1 Registro del Administrador y del operador

Objetivo

Registrar eventos y generar evidencias.

Aplicabilidad

Estas son políticas que aplican a la rectoría, coordinadora, Jefes de área, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de la organización.

Directrices preventivo o correctivo.

- ✓ Todos los funcionarios de Redp deben registrar y generar evidencia del mantenimiento a realizado.
- ✓ Todos los funcionarios de Redp deben hacer una lista de chequeo.
- ✓ El Colegio Luis Carlos Galan Sarmiento debe tener un historial ordenado, con copia de cada uno de los activos que se encuentran en cada sala de computo académica o administrativa

7.8 GESTIÓN DE ACTIVOS

7.8.1 Inventario de Activos

Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.

Directrices

- ✓ Se debe mantener un inventario de los activos existentes en la institución.
- ✓ Se debe tener identificado los activos que tiene la institución.
- ✓ Se debe tener en el inventario únicamente el registro de los activos propios de la institución.
- ✓ Se debe identificar, documentar e implementar reglas claras para el buen uso de los activos.
- ✓ El docente debe entregar al finalizar el contrato un paz y salvo de todos los activos que utilizo durante su permanencia en la institución.

Objetivo: Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización

Directrices

- ✓ Se debe clasificar la información en confidencial, secreta, reservado o publica
- ✓ La información debe estar ordenada en carpetas con su respectiva clasificación de la información.

7.9 CONTROL DE ACCESO

7.9.1 Requisitos del Negocio para el Control de Acceso

Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información

Directrices

- ✓ Los estudiantes no podrán ingresar a cuenta de administrador
- ✓ Nadie tiene permisos autorizados para ingresar a la página web sobre acceso contable, solo la persona encargada de dicha labor.
- ✓ Cada docente debe tener un usuario y clave de acceso al sistema que se encuentra en las salas de tecnología académicas.
- ✓ Los nombres de los usuarios deben tener su primer nombre punto apellido.
- ✓ Se debe eliminar el usuario cuando ya no pertenezca a la institución.
- ✓ La clave de los usuarios deben tener como mínimo 8 caracteres y debe contar con números y letras.
- ✓ Los administradores deben revisar cada 8 días las claves de los usuarios.

- ✓ Los usuarios deben cambiar periódicamente la contraseña.

7.10 SEGURIDAD DE LAS OPERACIONES

7.10.1 Procedimientos operacionales y responsabilidades.

Objetivo: Asegurarse de la integridad de los sistemas operacionales.
Directrices

- ✓ La empresa encargada de generar los boletines al colegio debe tener la seguridad necesaria para conservar los boletines.

- ✓ La institución deberá crear formatos para los diferentes procedimientos de operaciones y formatos para responsabilidades.

7.11 RELACIONES CON LOS PROVEEDORES

Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.
Directrices

- ✓ Acceso limitado a los recursos informáticos por parte de proveedores
- ✓ Revisar de manera constante los servicios prestados por los proveedores
- ✓ Generar responsabilidades en los aspectos relativos a la seguridad informática
- ✓ El colegio debe elaborar un contrato con el proveedor
- ✓ El contrato debe contener derechos, deberes y responsabilidades, estar sujeto a la ley y posibles sanciones por incumplimiento.
- ✓ El colegio Luis Carlos Galán Sarmiento debe entregar al contratista y a sus trabajadores su respectivo carnet con fecha de Inicio y finalización del contrato.

7.12 CONTRATOS

Objetivo

Cumplir con la cláusula del contrato y seguridad de la información.

Aplicabilidad

Estas son políticas que aplican a contratistas y proveedores.

Directrices

- ✓ Dentro de las cláusulas del contrato es importante mencionar la importancia de algunos activos informáticos que deben ser protegidos
- ✓ Mencionar las políticas de seguridad que tiene el colegio con la información que va a manejar.

- ✓ Cumplir con las clausulas establecidas en el contrato
- ✓ Cumplir con el tiempo asignado para dicho trabajo
- ✓ Retención documental de la contratación, actividad contractual
- ✓ Si el contrato con persona Natural es importante la copia del Rut y fotocopia de la cedula.
- ✓ Para persona Natural o jurídica es importante el Certificado de la cuenta a su nombre donde pretendería que le sean transferidos los pagos
- ✓ Cláusula de confidencialidad, integridad y disponibilidad de la información.
- ✓ La liquidación del contrato se llevara a cabo cuando se ha cumplido con todas las obligaciones y actividades pactadas.
- ✓ Confiabilidad que no se divulgue la información de acuerdo a lo establecido en la ley 1273 de 2009 y 1581 de 2012.
- ✓ En caso de cualquier eventualidad por parte del proveedor, éste debe notificarlo por escrito y entre las partes realizar un acuerdo a lo pacto en el contrato inicial.

RECOMENDACIONES

- ✓ Es de vital importancia manejar en el Colegio Luis Carlos Galán sarmiento un manual de Políticas de Seguridad informática para proteger los activos de la institución, supervisar el bienestar informático y ética de los usuarios.

- ✓ Las Políticas de seguridad establecidas en ésta monografía pueden ser aplicadas en otra institución distrital con las mismas características a ésta.

- ✓ Para la Política de seguridad el activo más significativo es la informaciòn; por ello es de vital importancia la capacitación de los usuarios con todo lo relacionado con seguridad informática.

- ✓ Se recomienda al Colegio que es importante asignar roles a los usuarios teniendo en cuenta su perfil, para así brindar mejor uso a sus componente tecnológicos, información importantes y toda la infraestructura de sistemas que se encuentra instalada.

- ✓ Cumplir con las políticas y normas de seguridad registradas en éste documento para evitar perdida de información.

- ✓ Rotular información de acuerdo a esquemas de clasificación.

- ✓ Se le recomienda al personal administrativo, docentes y estudiantes que es importante no abrir correos desconocidos.

- ✓ Evitar violaciones a las normas establecidas por la institución educativa y las leyes.

- ✓ Cuando el usuario se levante del computador, cerrar las sesiones del correo electrónico y páginas sociales, pues esto ocasionaría perdida de información.

CONCLUSIONES

- ✓ La implementación del SGSI es beneficioso para la Comunidad en cuanto a: seguridad efectiva en los sistemas de información; mejoras continuas en procesos de auditorías internas dentro de la Comunidad; incremento de la confianza en la Comunidad y mejora de su imagen.

- ✓ Actualmente en la sociedad de la información, es necesario que todas las organizaciones, sin tener en cuenta su tamaño, implementen mecanismos que permitan mantenerla segura, donde una se use la norma internacional ISO/IEC 27001 como un sistema basado en procesos que busca garantizar la seguridad de la información, siguiendo una serie de pautas y controles que de aplicarse, minimizan los riesgos a los cuales se ve expuesta.

- ✓ Verificar la situación actual de una entidad es importante, pues busca conocer lo que tiene a nivel de sistemas, como se estructura, su misión, su visión, todos sus activos informáticos, clasificación de éstos activos e impactos o valoración de daño que puede ocasionar al colegio Luis Carlos Galán Sarmiento.

- ✓ Con la infraestructura tecnológica del Colegio Luis Carlos Galán Sarmiento se visualiza su contenido tecnológico y las pautas que se puede aplicar para proteger los activos mediante un estudio de Seguridad Informática.

- ✓ El identificar amenazas y vulnerabilidades sirve como alerta para implementar la seguridad de la información a los activos que presentan riesgo dentro de la institución.

- ✓ La clave para proponer seguridad de la información esta concadenado por 3 elemento a saber: políticas, estándares y procedimientos de seguridad.

- ✓ Con el desarrollo y culminación del proyecto se logró determinar la terminación de todos los objetivos planteado, dando como resultados el proponer políticas de seguridad de la información para la institución educativa Luis Carlos Galán Sarmiento.

BIBLIOGRAFIA

- ✓ CASTRO Alfonso Favián & Díaz Verano, Fabián A. Análisis De Vulnerabilidades A Nivel De Acceso Lógico Basado En La Norma ISO/IEC 27001 En La Comunidad Provincia De Nuestra Señora De Gracia De Colombia. Proyecto de Grado, Ingeniería de Sistemas, Fundación Universitaria Konrad Lorenz. Bogotá, Colombia 2010.

- ✓ GOBIERNO DE ESPAÑA. Magerit - versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro II - Catálogo de elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

- ✓ HURTADO DE BECERRA, Jacqueline. Metodología de la investigación holística. Caracas Venezuela, Edit. Sypal. 2000. Pág. 18. (En el pdf suministrado se encuentra en la página 36).

- ✓ ICONTEC.Instituto Colombiano de Normas Técnicas y Certificación. Compendio: Sistema de Gestión de la Seguridad de La Información: SGSI. Bogotá. 2006

- ✓ MARCOMBO, Alexander. Diseño De Un Sistema De Seguridad Informática. Alfaomega. México, 2007.

- ✓ SEGUNDA COHORTE DEL DOCTORADO EN SEGURIDAD ESTRATÉGICA. Seguridad de la Información. En: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica, 2014, No. 1, p 15-16

WEBGRAFIA

- ✓ ANGEL, L., & Encimas, V. (s.f.). Politica Empresarial. Recuperado el 27 de Noviembre de 2013, de http://politicaempresarialfaca.blogspot.com/

- ✓ ALVAREZ, Daniel. Seguridad en Informática. [en línea]. En: Maestro en Ingeniería de sistemas empresariales. p.7. [citado el 24-05-17].Disponible en http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

- ✓ ALVAREZ, Jerzon. Diseño De Un Sistema De Gestión De Seguridad De La Información - Sgsi Basado En La Norma Iso27001 Para El colegio pro-colombiano de la ciudad de Bogotá, que incluye: asesoría, planeación. Proyecto de grado del área del Conocimiento - Gestión de la Seguridad Informática: Área Específica: SGSI basado en ISO27000 e ISO27001. Bogotá, D.C. Universidad Nacional Abierta Y A Distancia (Unad).

- ✓ AulaUrbana. Redp: Logros en infraestructura, conectividad y calidad. [en línea] [citado el 03-12_2017]. Disponible en: file:///C:/Users/ZAIRA/Downloads/585-Texto%20del%20art%C3%ADculo-1117-1-10-20160607%20(3).pdf

- ✓ AREITO, Javier. Seguridad de la Información: Redes, informática y sistemas de información. Editorial Paraninfo, 2008.p.54

- ✓ AUDISIS. Sistema de gestión de seguridad de la información - SCSI ISO 27001:2013 - Implantación y auditoría. [en línea]. Bogotá. Disponible en: http://www.audisis.com/BROCHURE_Sem_Implementaci%C3%B3n_SGSI.pdf

- ✓ BEEKMAN, George. Seguridad Informática. [online]. 1994. [citado el citado 01-06-2017]. Disponible: http://problema.blogcindario.com/2008/10/00014-marco-teorico.html

- ✓ BENITEZ, Moisés. GESTION INTEGRAL: Políticas de Seguridad Informàtica.2013. [en línea]. [citado el 2-06-17]. Disponible en http://www.gestionintegral.com.co/wp-content/uploads/2013/05/Pol%C3%ADticas-de-Seguridad-Inform%C3%A1tica-2013-GI.pdf

- ✓ CENTRO NACIONAL DE APRENDIZAJE. Estándares para la seguridad de información: Historia [en línea] SENA. [citado el 25-05-17]. Disponible en: https://senaintro.blackboard.com/bbcswebdav/institution/semillas/217219_1_VIRTUAL/OAAPs/OAAP1/aa1/oa_estandarseguridad/oc.pdf

- ✓ Cloud SecurityServices. Seguridad para todos. [citado el 24-05-17]. Disponible en http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html

- ✓ COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (Diciembre 31 de 2008). Diario Oficial 47.219 de diciembre 31 de 2008. p. 1-15.

- ✓ COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 57 de 1985 (julio 5 de 1985). Bogotá. Diario Oficial 05 de julio de 1985. p. 1-6.

- ✓ CUERVO, J. Aspectos Jurídicos de Internet y el comercio electrónico. (en línea). (7 de Junio de 2017)Recuperado de :http://www.informatica-juridica.com/trabajos/Aspectos_juridicos_de_Internet_y_el_comercio_electronico.asp

- ✓ COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (05 de enero de 2009). Bogotá. Diario Oficial 47.223 de enero 5 de 2009. p. 1-15.

- ✓ COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1266 gi(diciembre 31 de 2008 Bogotá. Diario Oficial 47.219 de 31 de diciembre de 2008. p. 1-19.

- ✓ COLOMBIA. CONGRESO DE LA REPÚBLICA. Decreto 1377 (27 de junio de 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Diario Oficial 48.834 de 27 de junio de 2013. p. 1-11.

- ✓ COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1266 (julio 30 de 2009). Bogotá. Diario Oficial 47.426 de julio 30 de 2009. p. 1-34.

- ✓ COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1581 (octubre 17 de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial 48.587 de octubre 18 de 2012. p. 1-15.

- ✓ Córdoba Martha. Tipos de Investigación. Disponible en: http://2633518-0.web-hosting.es/blog/didact_mate/9.Tipos%20de%20Investigaci%C3%B3n.%20Predictiva%2C%20Proyectiva%2C%20Interactiva%2C%20Confirmatoria%20y%20Evaluativa.pdf

- ✓ Colegio Luis Carlos Galan Sarmiento. Proyecto de Vida Galanista. Recuperado de: http://www.colegioluiscarlosgalansarmiento.edu.co/index.php?lang=es

- ✓ DUTRA, Enrique. Seguridad Informática. [online]. 2017. [citado el 26-11-2017]. Disponible: https://enriquedutra.wordpress.com/

- ✓ GÓMEZ G., Yessica. Seguridad de la información [en línea]. s.l.: Slideshare, 2013. [citado el 07/06/2017]. Disponible en: http://www.csiete.org/

- ✓ GOBIERNO DE ESPAÑA. Magerit - versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro II - Catálogo de elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

- ✓ GONZALEZ, DanielF. EL RIESGO Y LA FALTA DE POLITICAS DE SEGURIDAD INFORMÁTICA UNA AMENAZA EN LAS EMPRESAS CERTIFICADAS BASC. Administración de la seguridad y salud Ocupacional. [en línea]. [citado el 2-06-17]. Disponible en http://repository.unimilitar.edu.co/bitstream/10654/12251/1/ENSAYO%20FINAL.pdf

- ✓ HERNANDEZ, Marisol. Metodología de la Investigación. Disponible en: http://metodologiadeinvestigacionmarisol.blogspot.com.co/2012/12/tipos-y-niveles-de-investigacion.html

- ✓ HURTADO DE BARRERA, Jacqueline. Guía para la comprensión holística de la ciencia. 3a ed. Caracas: Fundación Sypal, 2010. p. 132.

- ✓ ICETEX. Instituto Colombiano De Crédito Educativo Y Estudios Técnicos En El Exterior Manual De Políticas De Seguridad De La Información. [en línea]. [citado en 27 de Noviembre de 2017]. Disponible en: https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manualseguridadinformacion.pdf

- ✓ INSTITUTO COLOMBIANO DE NORMALIZACIÒN Y CERTIFICACIÒN. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. NTC-ISO-IEC 27001. Bogotá.: El Instituto, 2013. 37 p.

- ✓ ISO 27001. Sistema de gestión de la seguridad de la información [en línea]. Colombia 1995. [citado el 24-05-17]. Disponible en: http://www.sgs.co/es-ES/Health-Safety/Quality-Health-Safety-and-Environment/Risk-Assessment-and-Management/Security-Management/ISO-27001-2013-Information-Security-Management-Systems.aspx

- ✓ ISO 27000.ES. Glosario [en línea]. Madrid: El autor, s.f. [citado el 26-11-2017]. Disponible en: http://www.iso27000.es/glosario.html

- ✓ ISO 27000.ES. Glosario [en línea]. Madrid: El autor, s.f. [citado el 26-11-2017]. Disponible en: http://www.iso27000.es/glosario.html#section10a

- ✓ ISO 27000.ES. Glosario [en línea]. Madrid: El autor, s.f. [citado el 26-11-2017]. Disponible en: http://www.iso27000.es/glosario.html#section10d

- ✓ ISO 27000.ES. Sistema de gestión de la seguridad de la información [en línea]. Madrid.Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

- ✓ MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Catálogo de Elementos, Página 7,22 [Consultado 24/05/2017], disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

- ✓ MARTOS, Fernando. Centros Hospitalarios de Alta Resolución de Andalucía-Auxiliares Administrativos. Primer Edición. España.2006. 195 p. Recuperado de: https://books.google.com.co/books?id=SmwP1cZdI4cC&pg=PA195&dq=LA+METODOLOG%C3%8DA+MAGERIT+3.0&hl=es&sa=X&ved=0ahUKEwiK5d7u_KTJAhUJWCYKHadoB14Q6AEIJTAC#v=onepage&q=LA%20METODOLOG%C3%8DA%20MAGERIT%203.0&f=false

- ✓ MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Fortalecimiento de la gestión TI en el estado [en línea]. Bogotá. http://colnodo.apc.org/apropiacionTecnologias.shtml

- ✓ PERAFÁN , Jhon. Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. [en línea]. [citado en 27 de Noviembre de 2017]. Disponible en: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2655/3/76327474.pdf

- ✓ WORDPRESS. Gestión de Riesgos en la Seguridad Informática. Citado el 07 de Junio de 2017. Internet: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

- ✓ WHITTEN, Jeffrey. Seguridad Informática. [online]. 1994. [citado el citado 01-06-2017]. Disponible: http://problema.blogcindario.com/2008/10/00014-marco-teorico.html

- ✓ 1 Términos de uso información iso27000.es. ISO 27000.ES. Historia. [en línea]. [citado el 25-05-17]. Disponible en: http://www.iso27000.es/iso27000.html

- ✓ UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Políticas de Seguridad: Definición de Política [en línea]. UNAM. [citado el 24-05-17]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/DefinicionPolitica.php

- ✓ ISMS. La importancia de contar con una política de seguridad en la empresa. [citado el 24-05-17]. Disponible en http://www.protegetuinformacion.com/perfil_tema.php?id_perfil=7&id_tema=63

- ✓ SOFTWARE DE GESTIÓN PARA LA EXCELENCIA EMPRESARIAL. Enero 13 de 2015. [en línea]. ISOTools. [citado el 2-06-17]. Disponible en: https://www.isotools.org/2015/01/13/iso-27001-pilares-fundamentales-sgsi/

- ✓ JARAMILLO, A. Manual de derecho de autor. (en línea). (7 de Junio de 2017). Disponible en: http://www.derechodeautor.gov.co/documents/10181/331998/Cartilla+derecho+de+autor

- ✓ 1 COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527 (18 de agosto de 1999). Bogotá. Diario Oficial 43.673 de 21 de agosto de 1999. p 1-2.

- ✓ El portal de ISO 27001 en español. Disponible en: http://www.iso27000.es/

- ✓ SGSI. Sistema de Gestión de Seguridad de la Información. [online]. 2017. [citado el 26-11-2017]. Disponible: http://www.pmg-ssi.com/2015/06/iso-27001-vulnerabilidades-de-la-organizacion/

- ✓ 1 DEFINICIÓNABC. Definición de confidencialidad. . [online] s.l.: El autor, s.f. [citado el 26-11-2017]. Disponible en: http://www.definicionabc.com/comunicacion/confidencialidad.php

- ✓ MINISTERIO DE EDUCACIÒN NACIONAL. [online]. república de Colombia. [citado el 26-11-2017]. Disponible en: http://www.mineducacion.gov.co/1621/article-79361.html

- ✓ UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Políticas de seguridad informática de la organización [online]. México: UNAM, s.f. [citado el 26-11-2017]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap4.html

- ✓ URECHE, Manuel. Diseño de políticas de seguridad informática basadas en la norma ntc-iso-iec 27001:2013 para la universidad de Cartagena centro tutorial mompox bolívar. Universidad nacional abierta y a distancia unad especialización en seguridad informática. [en línea]. [citado en 27 de Noviembre de 2017]. Disponible en: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/12027/1/19772159.pdf

- ✓ Secretaria de Educación del Distrito. Presentación contable fondos de servicios educativos. [en línea]. [Citado el 03-12-17]. Disponible en: http://www.educacionbogota.edu.co/archivos/Temas%20estrategicos/FSE/2013/PRESENTACION_CONTABLE_FONDOS_DE_SERVICIOS_EDUCATIVOS.pdf

- ✓ SIGEPRE. Presidencia de la república. Guía para la calificación de la información de acuerdo con sus niveles de seguridad. [en línea] [citado el 04-12_2017]. Disponible en: http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/G-GD-02-calificacion-informacion.pdf