CREACIÓN E IMPLANTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BAJO EL ESTÁNDAR ISO/IEC 27001:2013 PARA LA INSTITUCIÓN EDUCATIVA LUIS CARLOS GALÁN DE VILLAGARZÓN PUTUMAYO

JAIRO HERNANDO QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA

PITALITO, HUILA

2015

CREACIÓN E IMPLANTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BAJO EL ESTÁNDAR ISO/IEC 27001:2013 PARA LA INSTITUCIÓN EDUCATIVA LUIS CARLOS GALÁN DE VILLAGARZÓN PUTUMAYO

Tesis de grado para optar por el título:

Especialista En Seguridad Informática

Director de Proyecto:

Erika Liliana Villamizar Torres

Ingeniera de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA

PITALITO, HUILA

2015

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Santafé de Bogotá, 26 de septiembre de 2015

TABLA DE CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

RESUMEN

Este trabajo está orientado a la creación del SGSI para la institución educativa Luis Carlos Galán de Villagarzón Putumayo, con el propósito de salvaguardar los activos de la entidad, se recogen aspectos relevantes del tema iniciando con un análisis de vulnerabilidades a través de distintos métodos de pentesting y se prolonga en los distintos servicios que se ofrecen, con el propósito de tener bases para determinar los riesgos y amenazas de todos sus activos vinculados.

Con esta información de insumo, se inicia el proceso de creación del SGSI, estableciendo las salvaguardas y controles con el propósito de minimizar los riesgos y amenazas, así como también de buscar en algunos casos eliminarlos.

Todo el proceso se hace para cada componente de activos, también con el visto bueno de las directivas de la institución e involucrando a todo el personal en el objetivo general del proyecto.

Finalmente se crean las políticas según cada componente detectado en los activos y en los puntos anteriores y luego de un análisis minucioso de los riesgos categorizados según la metodología Magerit 3.0.

También se orientan formatos en distintos niveles para la entidad que sirven para darle organización a los procesos internos y así mismo el proceso de auditoría para hacerle seguimiento al SGSI.

PALABRAS CLAVE: SGSI (Sistema de Gestión de Seguridad Informática). Pentesting. Vulnerabilidad. Riesgos. Amenazas. Activos. Política. Magerit. Auditoría.

INTRODUCCIÓN

Hoy en día la mayor parte de las organizaciones tanto públicas como privadas gozan de Sistemas de Información, redes de datos y dispositivos electrónicos para manejar los datos en torno a cumplir los objetivos de la empresa.

El manejo de información abarca muchos aspectos como archivo, documentación, correspondencia, Sistemas de Información internos y externos. Las instituciones educativas como el colegio Luis Carlos Galán de Villagarzón, tratan información personal y académica de los estudiantes, padres de familia, docentes y comunidad educativa, con la falencia de que no tienen un control ni prevención ante posibles amenazas de pérdida de información o acceso abusivo y daño de sus sistemas informáticos entre otros riesgos que evidencian la necesidad de implementar un sistema de gestión de seguridad de la información o medidas informáticas que permita prevenir y controlar estas insolvencias.

Con el desarrollo de este proyecto se pretende concientizar y cambiar la falsa percepción de que esta tarea de cuidar o salvaguardar la información es solo de expertos o ingenieros de sistemas, ya que se propondrá un modelo de implementación del sistema de gestión de seguridad de la información, donde se abordarán temas como el análisis de riesgos, las políticas de seguridad, controles, auditorías y las responsabilidades de toda la comunidad educativa involucrada. Se iniciará con el conocimiento de la institución y sus objetivos, pasando por el análisis de riesgos a través de las vulnerabilidades encontradas y conociendo sus fortalezas y debilidades, para encaminarla hacia la creación de unos controles adecuados y normalizados a través de su SGSI y con un sistema eficiente de monitoreo y auditoría interna para su respectivo seguimiento.

La institución educativa Luis Carlos Galán conforme a sus demás políticas de crecimiento, inclusión de TIC y desarrollo, también busca las buenas prácticas en cuanto a seguridad de la información.

1. FORMULACIÓN DEL PROBLEMA

La Institución Educativa Luis Carlos Galán ha implementado algunos servicios informáticos para mejorar sus procesos, procedimientos y ofrecer una mejor atención a la comunidad, actualmente no se evidencia la importancia que debe dársele a la seguridad informática para proteger los activos de información existentes, por lo cual se está dando continuidad a los problemas actuales sobre ataques efectuados y lo peor, aquellos que podrían realizarse en el futuro, explotando las vulnerabilidades que tienen sus sistemas.

No proteger la información es exponer a la institución en general porque tiene el valor y activo más importante para el colegio, una ruptura en la seguridad puede dar el caso que un estudiante cambie sus calificaciones y a la vez los reportes o un caso más relevante, se pierda la información.

El resguardo seguro de los datos es el punto esencial en el proceso de tratamiento electrónico, así mismo contar con la información eficaz y precisa en el momento que se requiere, es la base para mantener la fluidez en los objetivos de la institución.

Los riesgos en el control de información a través de las plataformas implementadas siempre deben reevaluarse, auditarse y aplicarse políticas de control, la institución educativa objeto del presente trabajo aún no cuenta con un sistema que le permita mantener seguro su principal activo, la información, apegándose únicamente a sistemas de seguridad comunes que no siempre garantizan los resultados, sin que existan una responsabilidad a cargo de un profesional, de igual manera los usuarios no cuentan con la capacitación, conocimiento y responsabilidad al momento de interactuar con la base de datos, permitiendo accesos a personal ajeno a la institución y no autorizado, divulgación de contraseñas, sistema de autenticación débil, entre otros problemas.

Por esta razón el señor rector, docentes y comunidad educativa, ven con preocupación que la información tenga cierto riesgo tanto la que está en la nube como la que se encuentra localmente, pero que tiene acceso remoto y se espera alguna solución para mejorar la seguridad de los servicios instalados a través del proyecto TIC de la institución, con el fin de darle continuidad al mismo; hasta el momento no se cuenta con políticas de seguridad ni con alguna capacitación a los docentes para el manejo de contraseñas, igualmente no se ha hecho auditoría ni seguimiento a todos los sistemas para ver qué tan seguros son ante cualquier ataque, la página web no cuenta con ningún sistema de protección o seguridad, sólo los básicos ofrecidos por el operador Hosting donde se aloja la página, la autenticación funciona de manera normal, sin tener mínimos requerimientos.

Finalmente cabe resaltar que de acuerdo a las políticas de la institución se proyecta ampliar las plataformas informáticas vía web para otros servicios, lo que implica mayores riesgos y vulnerabilidades por atender.

¿Los Sistemas de Información de la institución educativa Luís Carlos Galán de Villagarzón Putumayo se encuentran preparados para evitar o protegerse de cualquier ataque?

2. JUSTIFICACIÓN

Hoy encontramos que el desarrollo de la tecnología tiende hacia entornos web, con distintos servicios aplicados a través de software que se implementan para lograr ser utilizados desde cualquier punto de la red, es así como con la aparición de la web 2.0 y subsiguientes empezamos una nueva era en materia de información a través de webs dinámicas.

En la misma medida que observamos este gran desarrollo en internet y las redes de datos, también lastimosamente se encuentran los problemas de seguridad, originados por distintos ataques que vistos desde distintos ángulos no son sino la forma de acceder a nuestra información privada para aprovecharse de ella y cometer actos delincuenciales e ilícitos; día a día salen nuevas formas de atacar y explotar las vulnerabilidades de un sistema informático y esto ocasiona problemas a gran escala cuando no se está preparado para contrarrestarlos.

De aquí se parte la necesidad de hablar de seguridad, donde toda empresa debe involucrar su área o departamento de sistemas para mitigar todos los riesgos que sean visibles ante una posible amenaza y velar por la protección de la información, esto no solo implica los riesgos externos generalmente producidos por un atacante de la red, sino también por factores internos asociados a usuarios y personal de confianza.

La institución educativa Luis Carlos Galán cuenta actualmente con algunos servicios en la web y dos servidores locales, a los cuales también se les permite accesar por internet, pero no cuenta con políticas, normas internas o un sistema integrado de seguridad informática. En el colegio existe el departamento de Sistemas conformado por dos (2) digitadores o auxiliares y un (1) Ingeniero de sistemas que también presta los servicios como docente, a quien le recae la responsabilidad de la seguridad por no contar con otro profesional y además la Secretaría de Educación Departamental, organismo que fija el personal de nómina

Comentario [MCCR1]: Es mejor escrito acceder.

para este establecimiento educativo, no aprueba más administrativos de apoyo en esta área; por estas razones el Ingeniero debe ser docente e integrante del Departamento de Sistemas a la vez, dejándole una responsabilidad grande y que requiere el apoyo de políticas para que todos aporten en seguridad y compromiso.

Como existen diversas formas de protegerse y distintos métodos, bien sea implementados de manera personalizada como la adquisición de equipos y software para tal fin, se concibe la necesidad de implementar un sistema de gestión de seguridad de la información para la entidad, con el fin de mejorar y mantener la seguridad informática en la Institución Educativa Luís Carlos Galán de Villagarzón Putumayo, a partir de los servicios que actualmente tienen instalados en general.

Es de vital importancia proteger la información ya que es el patrimonio y el baluarte de la institución educativa, porque contiene los datos más relevantes como matrícula, calificaciones, recursos educativos digitales de todas las áreas, evaluaciones en línea entre otros.

Perder casualmente la información implicaría un retroceso enorme y pérdida de tiempo, pues volver a recuperar los datos se vuelve complejo, peor porque en el momento no hay políticas de todo el proceso de backups, seguridad y auditoría de los datos para hacerle frente a un eventual ataque informático o recuperación de datos, dado también que son sistemas que se utilizan día a día como en toda institución de educación, tal es el caso de un ataque perpetuado hace algunos meses donde el sistema de calificaciones quedó fuera de línea, preciso en el momento de hacer cierre al período escolar académico, esto implicó la necesidad de hacer una revisión de toda la base de datos y como resultado afortunadamente se logró recuperar, pero la entrega de informes académicos a padres de familia tuvo que ser pospuesta para un mes después de la fecha programada, obligando a modificar el calendario escolar y algunas quejas de la comunidad.

En otro de los casos se podría generar pérdida de información general, esto de no ser posible una supuesta recuperación de datos, conllevaría a tener que volver a subir al sistema toda la información, incluyendo datos históricos de años anteriores lo que también implica contratar personal para hacerlo, costos económicos y de igual manera que otros casos pérdida de tiempo, en alguna situación podrá ser difícil su restauración por el desorden en el archivo físico o situaciones adversas por el escaso personal administrativo del colegio.

Podemos decir claramente que la correcta prestación del servicio educativo en la institución depende en gran parte del buen funcionamiento de los Sistemas de Información existentes en la entidad, su caída, mal funcionamiento, pérdida de información, ocasionaría un caos general ya que la mayor parte de los procesos se encuentran automatizados en los servicios anteriormente descritos y justificados.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Crear e implantar un Sistema de Gestión de Seguridad Informática para la Institución Educativa Luís Carlos Galán de Villagarzón Putumayo, basado en los requisitos de la norma 27001:2013, para incrementar la confianza en los Sistemas de Información, reducir los riesgos y garantizar la confidencialidad, integridad y disponibilidad de la información en todos sus niveles.

3.2 ESPECÍFICOS

- Conocer la norma ISO/IEC 27001:2013 con el fin de apropiarse de los conceptos y metodología para aplicarla en la Institución Educativa Luís Carlos Galán de Villagarzón.

- Realizar un diagnóstico e identificar las vulnerabilidades y amenazas de seguridad de información de los servicios, procesos y activos de la entidad, para cerrar las brechas.

- Analizar los riesgos existentes en la institución como base para el SGSI.

- Identificar y analizar los objetivos y requerimientos de seguridad del Sistema de Información de la institución para acoplarse con el nuevo método óptimo a crear.

- Buscar y crear los controles necesarios para tratar los riesgos mediante la creación de un plan de tratamiento.

- Formalizar el SGSI, mediante la documentación de las políticas, programas y procedimientos necesarios para gestionar los riesgos de seguridad de información de la institución.

- Ejecutar una autoría interna del SGSI después de su implementación, con el fin de tener resultados que puedan servir de comparación entre lo actual y la situación anterior a la implantación.

4. MARCO REFERENCIAL

Nuestra principal fuente es la norma ISO/IEC 27001 versión 2013, que contiene los lineamientos necesarios para implementar el SGSI, también sirve de referencia la Norma Técnica Colombiana NTC-ISO/IEC 27001 del año 2006, que es la misma norma anterior pero adaptada a procesos en nuestro país por ICONTEC.

Existen casos de éxito de universidades y entidades colombianas y europeas principalmente que han realizado implementaciones de Sistemas de Gestión de Seguridad de la Información y recomiendan algunos tips como: documentar el SGSI, exigir el debido cumplimiento de los procesos y procedimientos establecidos, realizar revisiones periódicas del mismo y sensibilizar al personal de la importancia de la seguridad de la información y demás temas relacionados.

En la búsqueda de información relacionada a través de internet, es preciso hablar de varias tesis de grado sobre el tema, particularmente encontramos el trabajo de Jorge Cástulo Guerrón Eras de la UOC de Máster Interunivesitario en Seguridad de las Tecnologías de Información y las Comunicaciones, denominado "Elaboración de un plan para implementación del sistema de gestión de seguridad de la información. Un portal que contiene información sobre tesis de grado relacionadas con seguridad de la información llamada **segu.info"**[1] de Argentina, con documentos importantes que sirven de base para varios aspectos a tener en cuenta en el presente trabajo.

Manual de Metodología Abierta de Testeo de Seguridad (OSSTMM), es uno de los estándares profesionales más completos y utilizados en auditorías de seguridad, sirve para revisar la seguridad de los sistemas desde internet, incluye un marco de trabajo aplicable con las fases que se deben realizar para la ejecución de la auditoría, este manual ha tenido éxito por la constante evolución.

[1]Tomado de consulta web: http://www.segu-info.com.ar/tesis/

Esta metodología libre permitirá contar con los lineamientos esenciales a la hora de efectuar la auditoría en uno de los pasos en la implantación del SGSI de la Institución Educativa Luís Carlos Galán.

Magerit es otra metodología libre para el análisis de activos y gestión de los Sistemas de Información, se utiliza la versión 3.0 junto con sus anexos y libro de catálogos, a través del software PILAR que se distribuye pero su licencia es de pago, dando la posibilidad de utilizar su demo por un mes.

En la fase de búsqueda de vulnerabilidades se pueden hacer pruebas de intrusión, para este proceso es posible hacerlo con un software completo denominado Kali Linux, ya que contiene varias herramientas para todo tipo de pruebas como testing bien sea a bases de datos, páginas web, redes y sistemas operativos, en general se puede encontrar información como manuales y videos de ayuda para utilizar esta suite, cuyos resultados serán un componente importante para el presente trabajo.

El Ministerio de Tecnologías de la Información y las Telecomunicaciones en Colombia también se ha unido para crear un modelo de seguridad para las entidades del Estado para que sirva como guía para construir el Sistema de Gestión de Seguridad de la Información; a través de su web se ofrecen los lineamientos para cumplir el objetivo.

Los portales relacionados con las normas más importantes se convierten en otra fuente de información para el presente trabajo, un ejemplo es: http://www.iso27000.es/herramientas.html

Como ejemplo de modelo e implantación de un SGSI se analizó el aplicado al Instituto Nacional de Tecnologías de Información de España (antes INTECO, hoy INCIBE).

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

4.1 ANTECEDENTES DE LA NORMA 27001

La norma BS 7799 de BSI apareció por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas, para la que no se establecía un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que estableció los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS 7799-2, esta norma se publicó por ISO, con algunos cambios, como estándar ISO 27001. Al tiempo se revisó y actualizó ISO 17799. Esta última norma se renombró como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

En Marzo de 2006, posteriormente a la publicación de ISO 27001:2005, BSI publicó la BS 7799-3:2006, centrada en la gestión del riesgo de los Sistemas de Información.

Asimismo, ISO ha continuado, y continúa aún, desarrollando otras normas dentro de la serie 27000 que sirvan de apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001, que es la norma principal y única certificable dentro de la serie.

En la actualidad está vigente la ISO/IEC 27001 versión 2013, con un total de 14 dominios y 113 controles, además de contar con nuevos controles de seguridad.

4.2 MARCO LEGAL

Muchas empresas de carácter público, especialmente las instituciones educativas no cuentan con ingresos económicos suficientes para invertir en seguridad informática, peor aún porque la contratación de honorarios y personal la hace según la ley 715 de 2012 directamente el ente certificado en cada región, para este caso la Secretaría de Educación del Putumayo; situación que hace más difícil invertir en personal idóneo para las labores de ayudar a proteger la información.

La institución educativa Luis Carlos Galán para poder mitigar este problema utiliza el personal nombrado con el que cuenta actualmente, asignando otras funciones complementarias.

La Ley 1273 de 2009 sobre delitos informáticos y protección de la información en Colombia.

Ley de Habeas Data 1581 de 2012, su decreto reglamentario 1377 de 2013, donde se reglamenta el uso, actualización y eliminación de información personal, junto con sus siete (7) ítems.

4.3 MARCO CONTEXTUAL

4.3.1 Nombre de la empresa. Institución Educativa Luis Carlos Galán

4.3.2 Reseña Histórica. Hace 17 años nació la Institución Educativa Luis Carlos Galán bajo la modalidad de escuela a nivel de primaria pública, luego fue ampliando su infraestructura poco a poco hasta alcanzar espacio para ofrecer educación de básica primaria, básica secundaria y media; El 28 de julio de 1997 la institución del municipio cambia de razón social por Colegio Técnico Luis Carlos Galán, mediante la resolución No 0154 del julio 28 de1997.

Según resolución número 0602 de diciembre 06 del año 2002 el colegio técnico Luis Carlos Galán se fusionó con los centros educativos:

- Escuela urbana mixta julio Garzón moreno
- Escuela urbana mixta cristo rey
- Escuela urbana mixta los diamantes

Desde el año 2012 se cuenta con más de mil estudiantes entre las tres sedes, en la Central hay estudiando 866 y el resto en las otras dos sedes, la institución cuenta con un sistema de evaluación vía web, blogs, periódico digital, laboratorios de física, química e informática, también con un espacio los días jueves de 2 a 3 de la tarde en la emisora comunitaria donde se comparten notas sobre educación y se está gestionando la construcción de dos o tres nuevos salones de clase porque los necesita en la sede central.

4.3.3 Misión. Tiene como principio fundamental proporcionar una educación integral al estudiante y de calidad donde se le permita desarrollar sus valores como persona. Para lograrlo el Colegio cuenta con un grupo de docentes capacitados y con mucha voluntad de trabajo, de igual manera la participación de la comunidad en el proceso educativo y la dotación de mobiliario, equipos y ayudas educativas necesarias para mejorar la calidad de la educación.

4.3.4 Visión. La Institución proporcionará bachilleres con valores y conocimientos suficientes para desempeñarse en al vida diaria para quienes que por algunas razones no pueden continuar en el sistema educativo y con proyección a la superación para aquellos que estén en condiciones de seguir adelante en el progreso formativo e intelectual de la profesionalización.

4.3.5 Políticas administrativas. Dentro de las políticas a nivel interno, se cuenta con un plan de estudios el cual es revisado cada año para ser mejorado.

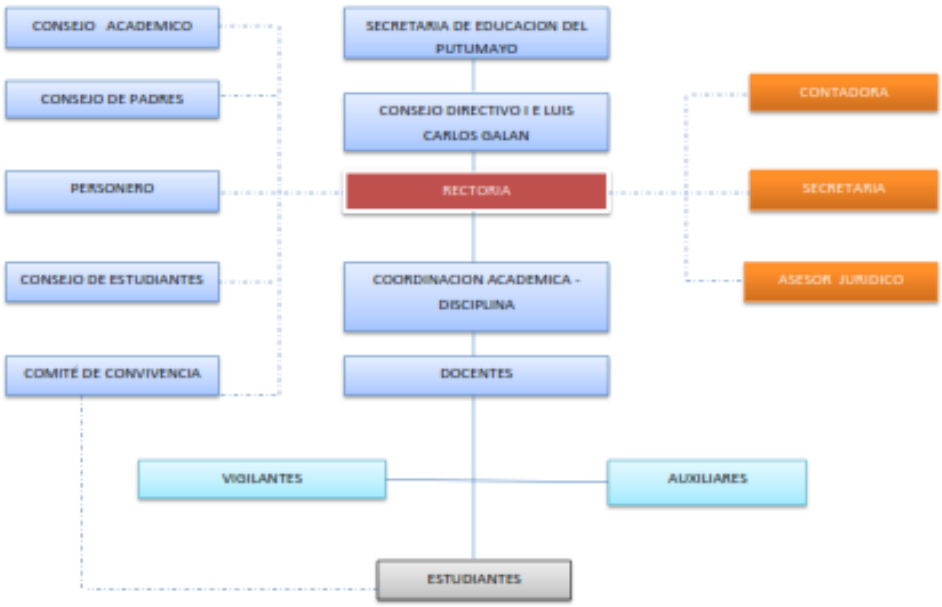
La institución funciona con el acompañamiento del consejo directivo para las actividades propuestas por el rector, también por el consejo académico quien colabora con las decisiones de tipo académico.

La institución viene adelantando una política de TIC encaminada hacia la utilización, capacitación e implantación de recursos mediados por tecnología; para este propósito se inició con el sistema de evaluación donde todos los docentes se ven obligados a utilizar un computador con navegador para subir los datos de matrícula y datos académicos del educando.

Se instalaron dos (2) servidores locales con plataformas virtuales para Inglés y las demás áreas, todos los docentes recibieron capacitación y actualmente y se cuenta con más de veinte (20) cursos creados de forma completa y se encuentran en uso por parte de docentes y estudiantes.

4.3.6 Organigrama Institucional

Figura 1. Organigrama Institución Educativa Luis Carlos Galán



Fuente: Secretaria Institución educativa

4.3.7 Permisos. Es conveniente solicitar permiso al señor rector y consejo directivo de la institución educativa Luís Carlos Galán para poder empezar el desarrollo de este proyecto, dando a conocer los objetivos del proyecto a realizar para tener acceso sin dificultad a todos los sistemas y a los procedimientos y demás documentación de la institución educativa.

5. RECURSOS DISPONIBLES

5.1 TALENTO HUMANO

Un ingeniero de sistemas, con experiencia en herramientas de pentesting, linux y búsqueda de vulnerabilidades, algunos docentes de la institución educativa que tienen conocimientos básicos en sistemas y desean participar en el proyecto una vez conocen el objetivo general y la problemática en seguridad de la institución.

Algunos estudiantes que hacen parte del grupo de investigación en informática de la institución para colaborar en los estudios previos.

También como líder general se encuentra el señor rector de la institución.

5.2 LOCATIVAS

La institución educativa cuenta además con sala de proyección para videos que puede ser utilizada para capacitaciones, también de una sala de reuniones completamente dotada con videobeam y silletería,

5.3 TECNOLOGÍA Y ACTIVOS

Se cuenta con dos salas de cómputo, portátiles y tablets para los docentes, igualmente conexión a internet alámbrica y wifi entre otros, que se mencionan en los ítems de activos y evaluación de los mismos del presente documento.

6. METODOLOGÍA DEL PROYECTO

En esta sección se describe la metodología propuesta para la implantación de un SGSI, organizado en las etapas de planificación del ciclo de mejora continua PHVA2 (Planear, Hacer, Verificar y Actuar), definido en la norma ISO/IEC 27001. Se presentan además diferentes alternativas de enfoque y estrategia, también se discute su conveniencia o no, para realizar el correspondiente análisis de riesgos y se complementó con la metodología Magerit, contemplado como punto inicial de los objetivos específicos.

Figura 2. Ciclo de mejora continua PHA

Fuente: http://mps1.minproteccionsocial.gov.co/evtmedica/linea%204/1.3phva.html

6.1 DISEÑO DE FASES PARA LA IMPLEMENTACIÓN DEL SGSI

A continuación se describen las fases o etapas para el SGSI en la institución educativa Luis Carlos Galán de Villagarzón.

[2] Blog explicativo de PHVA. Blog-Top Punto Com. [en línea]. http://www.blog-top.com/el-ciclo-phva-planear-hacer-verificar-actuar/

6.1.1 Primera fase. En esta etapa se hace el reconocimiento de todos los sitios y documentos necesarios para llevar a cabo el presente proyecto tales como:

- Diseño de la red de datos física y lógica
- Manuales de procedimientos
- Tipos de dispositivos con sus correspondientes manuales
- Manual de funciones de las personas encargadas de administrar los Sistemas de Información.
- Hojas de vida del personal encargado de seguridad de la institución.

6.1.2 Segunda fase. Se procede a analizar la finalidad de la institución educativa, teniendo en cuenta que se trata de tipo público y enfocada a atender toda clase de población en edad escolar de forma gratuita, es decir, no tiene fines lucrativos, luego se analizan los activos, estados del nivel de seguridad de los mismos.

- Visitas a las instalaciones locativas donde se encuentran los activos.
- Conocimiento de las políticas del firewall y proxy local.
- Funcionamiento de los servidores locales.
- Ingreso temporal a la cuenta de Cpanel del Hosting, para conocer más detalles de la página web y demás servicios instalados.
- Creación de cuentas de usuario de todos los Sistemas de Información tanto locales como remotos para realizar pruebas con el respectivo permiso.
- Documentación de la red, acceso temporal a todos los dispositivos de la misma para verificar su configuración y seguridad.

6.1.3 Tercera fase. Con todo lo anterior, más el ingreso temporal a los dispositivos y sistemas instalados, se procede a crear una serie de pruebas de testing con el fin de buscar vulnerabilidades en distintos niveles y servicios, con el propósito de determinar el grado de seguridad actual.

- Se procede a buscar y elegir las herramientas para realizar las pruebas, como primera medida se utiliza Kali Linux y su grupo de componentes, todos encaminados a realizar Pentesting y Ethical Hacking, también se utilizan herramientas en línea y otras pruebas directas basadas en la experiencia personal, todo aprovechando las bondades del software libre.
- Con las herramientas de escaneo y procediendo a utilizar otras de ataque de forma ética, se procede a verificar la respuesta a ataques como tipo diccionario, accesos no autorizados, vulneración de contraseñas, ping malicioso, revisión de puertas traseras, entre otros.
- Con los resultados se procede a verificar y darse una idea más clara de las vulnerabilidades en seguridad, se clasifican los activos para definir los controles o salvaguardas.

6.1.4 Cuarta fase. Finalmente se hace la implementación del SGSI en la institución objeto del estudio, formalizando las responsabilidades en la seguridad por sectores y teniendo en cuenta los controles propuestos.

- Implementación de los cambios propuestos y ejecución de controles.
- Capacitación y divulgación a docentes y administrativos.
- Responsabilidad para cada funcionario en el cumplimiento.
- Auditorías internas para verificar el SGSI.

7. DESARROLLO DEL PROYECTO

7.1 IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

7.1.1 Servidores. La institución cuenta con dos (2) servidores, uno con sistema Operativo Suse Linux Enterprise el cual tiene el servicio de plataforma virtual con Moodle, el hardware es una máquina normal con procesador Intel Xeon, disco duro de 1 Tera, 8 Gigas de memoria Ram, Board Intel y quemador de DVD. Este servidor contiene información de cursos, foros, evaluaciones y simulacros tanto de Icfes como preuniversitarios desde hace un año atrás, tienen acceso los estudiantes de bachillerato y los docentes.

El otro servidor es marca Lenovo, tiene sistema operativo Windows Server 2012 con licencia, procesador Intel Xeon, Ram de 8 Gb, disco duro de 1 Tera, se utiliza para el sistema virtual de bilingüismo desde hace un año.

7.1.2 Servicios en línea. La institución también ha invertido en software en línea para llevar algunos procesos como el de matrícula y registro de calificaciones de todos sus estudiantes llamado “Sigedin”; este se encuentra instalado en un servidor hosting de pago a través de la empresa Hosting 1ª y funciona permanentemente a través de sus diferentes módulos para estudiantes, padres de familia, docentes y directivos.

Se accede a través del dominio institucional y de la página web, también cuenta con un periódico digital en línea con información de los movimientos y noticias de la institución desde casi dos años atrás.

7.1.3 Equipos de cómputo. La sede central cuenta con dos (2) salas de cómputo equipadas con veintidós (22) computadores portátiles cada una, marca Lenovo y HP con procesador Celeron y 4 Gigas de Ram, acceso inalámbrico; adicionalmente a esto cada docente tiene un portátil asignado por parte del colegio para un total de cuarenta (40) y hay cinco (5) computadores más de oficina para Secretaria, auxiliar biblioteca, rectoría y coordinación.

En las sedes hay un promedio de quince (15) computadores por cada una entre PC de escritorio y portátiles, los cuales se usan para básica primaria de cuarto y quinto grado, estos están interconectados a la red central de la institución vía inalámbrica mediante Nano Station M5.

Se cuenta con dos switches de red de 24 puertos y dos (2) de 12 puertos, un router Mikrotik RB750.

También existen ciento sesenta (160) tablets marca Aprix.

7.1.4 Sistemas de seguridad. Solo se cuenta con seis (6) cámaras IP para el control de acceso a la sede con monitoreo desde la oficina de Coordinación.

7.1.5 Redes de datos. Existe una red cableada la cual conecta los dos servidores y las dos salas de cómputo, dos Wifi de buena potencia, una permite irradiar la señal a toda la institución a través de una NanoStation Loco M2 y la otra a través de tres (3) routers inalámbricos para conectar las tablets de la institución al servidor de bilingüismo.

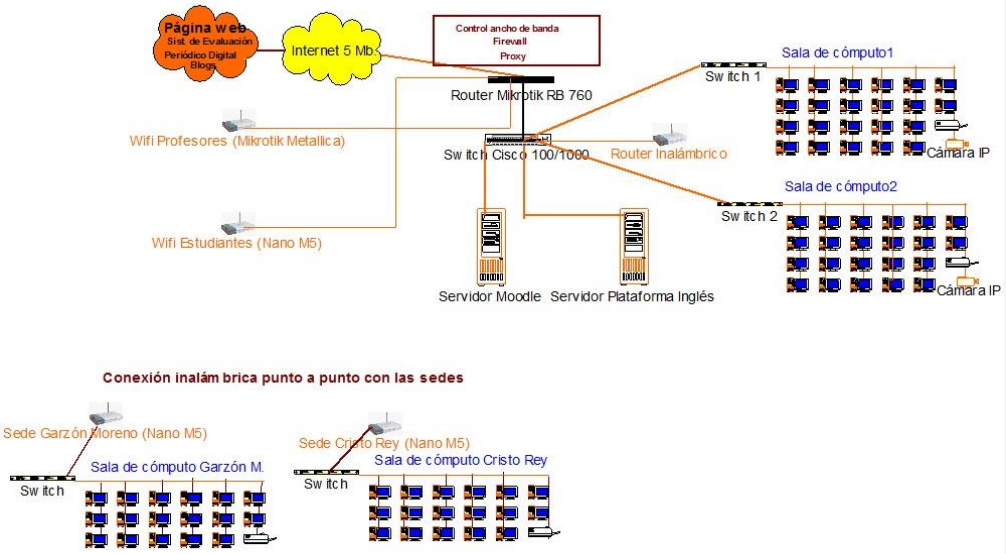
Las dos (2) sedes se conectan mediante una red inalámbrica punto a punto con NanoStation M5, con las salas de cómputo correspondientes para acceder a los servidores locales de la institución.

Dos canales de comunicación para Internet banda ancha, uno con capacidad de 4 Megas de bajada por dos (2) megas de subida para las dos salas de cómputo, el otro canal se utiliza únicamente para la parte administrativa de Secretaria, Coordinación y Rectoría el cual tiene dos megas de bajada por uno de subida.

La red es administrada desde un router Mikrotik administrable que tiene Firewall y Proxy incorporado, también cuenta con diferentes reglas de seguridad.

7.1.6 Diseño general de la red. A continuación se indica el diseño físico como se encuentra la red de la institución, permitiendo unir sus otras dos sedes.

Figura 3. Diseño red de datos I. E. Luis Carlos Galán



Fuente: Institución Educativa Luis Carlos Galán

7.2 ANÁLISIS Y RESUMEN DE LOS SISTEMAS MÁS IMPORTANTES PARA LA INSTITUCIÓN

7.2.1 Sistema de Gestión de Académica (SIGEDIN). Es el más importante ya que concibe el objetivo general de la institución, es un sistema adquirido a terceros, el cual se encarga de gestionar inscripciones, matrícula, docentes, padres de familia, directivos, biblioteca y todo lo relacionado con la parte académica de los estudiantes, incluyendo calificaciones, faltas y los reportes de comportamiento a través de su hoja de vida a lo largo de toda su vida en la institución.

Es un sistema vía web programado en PHP y MYSQL versiones actualizadas ya que cada año y medio aproximadamente se migra a una versión nueva tanto del gestor de bases de datos como de ajustes que se le hacen al sistema como tal.

Cualquier persona de la institución bien sea padre de familia, docente, directivo o estudiante desde cualquier terminal con usuario debidamente creado, puede acceder a esta herramienta para conocer información según corresponda,

También la secretaria general puede bajar información de la base de datos para subirla al SIMAT del Ministerio de Educación Nacional, esto genera la disminución de tiempo para preparar los formatos respectivos, igualmente es posible que un estudiante descargue su boletín, acceda a sus calificaciones vía web y baje sus constancias.

7.2.2 Plataforma Virtual Moodle. Corre de forma local bajo Suse Linux Enterprise versión 11 en uno de los servidores dedicados, está instalada la versión 2.8 con PHP, Apache y MYSQL, tiene licencia GPL y es uno de los sistemas de código abierto más usados en el mundo.

Actualmente cuenta con más de cuarenta (40) cursos para diferentes áreas como Lenguaje, Filosofía, Ética, Tecnología, Inglés, Sociales y Matemáticas; también tiene algunos cursos pre-icfes y pre-univesitarios con el fin de preparar a los estudiantes de décimo y once, en el futuro se pretende realizar cursos virtuales para padres de familia.

Esta plataforma se utiliza a través de los equipos ubicados en las salas de cómputo de la sede central y las otras dos sedes, también pueden acceder con celular por las redes Wifi tanto la de profesores, como de estudiantes respectivamente, también la institución cuenta con 160 tablets que se utilizan para ingresar a las dos plataformas virtuales también.

7.2.3 Plataforma Virtual Latin Campus. Es de licencia de pago donada por la Gobernación del Putumayo, se encuentra instalada en otro servidor dedicado marca Lenovo, corre bajo sistema operativo Windows Server 2012 con licencia, para su funcionamiento también tiene instalados IIS y Mysql.

Solo acceden los dos (2) docentes de Inglés con sus estudiantes, el curso ya está montado y cuenta con diferentes contenidos desde vocabularios, gramática, ejercicios en general incluyendo audios de Inglés, es una plataforma muy buena que ha dado resultados positivos en la enseñanza de esta materia para el proyecto de Bilingüismo.

8. ANÁLISIS DE VULNERABILIDADES

En este informe técnico se pretende identificar amenazas y vulnerabilidades que puedan ser explotadas de forma directa e indirectamente y causar daños al sistema, a la institución educativa y en si comprometer los activos de la misma.

Este escaneo se realizó con distintas herramientas de Ethical Hacking y posteriormente teniendo en cuenta la Metodología Magerit se realiza el análisis y gestión de los riesgos encontrados.

Se toman como referencia primero los servicios que actualmente presta y que forman parte primordial de los objetivos de la institución, donde es posible la presencia de fallos, robo, o modificación y que pueden comprometer seriamente la integridad de la información.

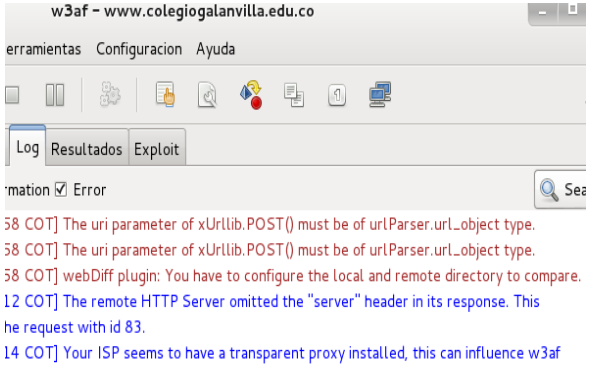
8.1 RESULTADOS ESCANEO DE VULNERABILIDADES

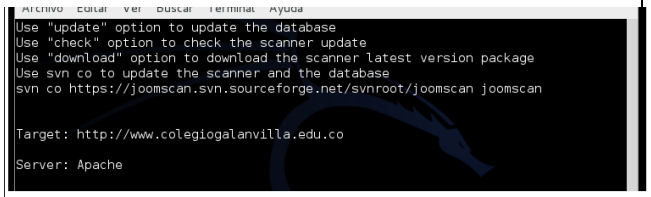
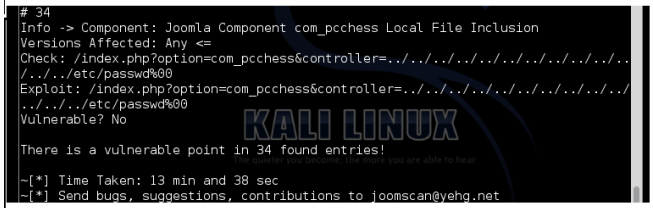
A continuación se muestran los resultados de la evaluación de los sistemas y dispositivos que forman parte de los activos de la institución educativa Luis Carlos Galán, con este informe se pretende establecer medidas de seguridad para:

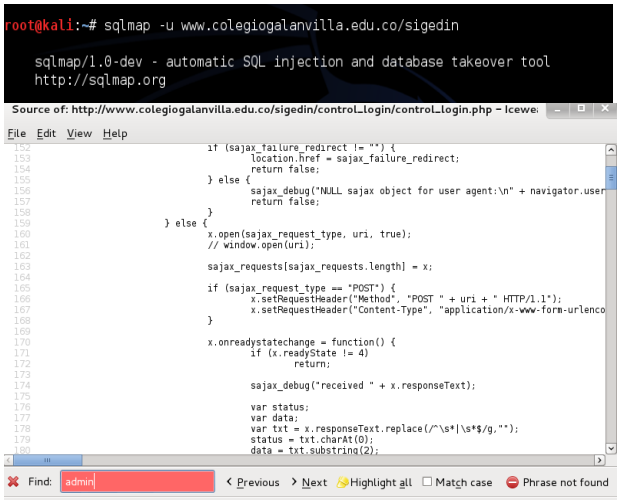
- Proteger la información de la red.
- Implementar y mejorar los controles implantados en el firewall, antivirus y demás dispositivos de la red.
- Establecer una política de seguridad de la información acorde a la institución educativa.

Tabla 1. Cuadro de escaneo de Vulnerabilidades

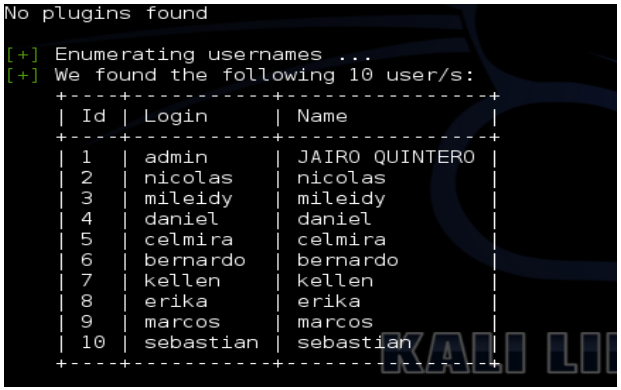
TIPO DE PRUEBAS	ACTIVO Y FECHA	CONCLUSIONES Y RECOMENDACIONES
1. Escaneo de puertos a los servidores. Se hizo el análisis con nmap y nslookup, se obuvo varios puertos abiertos en ambos servidores.  	Hardware Febrero 15/2015 Jairo Quintero	No existen políticas restrictivas para puertos ni a nivel de firewall, tampoco en cada servidor, de esta manera es fácil obtener información de uno de ellos. Se deben abrir solo los puertos 80, 25, 443 y 21 utilizados para http y ftp entre otros servicios, los demás puertos deben ser cerrados por seguridad. Se deben documentar políticas restrictivas de puertos tanto en el Firewall como en los servidores.
2. Análisis de vulnerabilidades a la página web.	Servicios Febrero 16/2015	A pesar de no tener vulnerabilidades conocidas, es necesario mantener el sistema CMS Joomla actualizado

Se hace primero con w3af de Kali Linux.   	Jairo Quintero	para evitar problemas. Las políticas de seguridad del servicio Hosting también ayudan a mejorar.

El bug fue detectado por la seguridad del Hosting y fue bloqueado. Como es una web basada en Joomla, se procede a utilizar el escáner de vulnerabilidades para este CMS específicamente llamada joomlascan de OWASP en Kali Linux.   Finalmente de las 34 entradas buscadas en Joomla, ninguna dio positivo como vulnerabilidad efectiva en la página.		
3. Análisis de vulnerabilidad y ataque al sistema de evaluación académica SIGEDIN.		El código como tal está bien programado y evita ataques tipo

Después de hacer un backup de todo el sistema, se intentó una prueba de inyección de sql con sqlmap.  El sistema está protegido para este tipo de ataques, en su código fuente podemos ver que no es posible encontrar código vulnerable donde se encuentre información de usuarios.		inyección sql, pero hay problemas en las reglas para las contraseñas, se deben crear para evitar que los usuarios ingresen con contraseñas débiles.
4. Análisis de vulnerabilidad web periódico	Servicios	Está basado en Joomla 2.5, es

escolar. También se usa joomscan porque el periódico está basado en Joomla versión 2.5.  Los resultados dieron negativo para vulnerabilidades, sin embargo la versión de Joomla no es la más reciente y esto puede atraer problemas futuros.	Febrero 16/2015 Jairo Quintero	conveniente actualizar a una versión más nueva como la 3x que mejora aún más la seguridad.
5. Análisis de vulnerabilidad web a blogs de la institución. Se usa la herramienta WPScan para buscar problemas de seguridad en WordPress de blogs.	Servicios Febrero 16/2015 Jairo Quintero	Crear la política de contraseña fuerte porque es vulnerable a ataque por diccionario o fuerza bruta, ya que el usuario es fácilmente detectable como ocurrió en la prueba.



El resultado fue positivo para encontrar usuarios, entre ellos el más importante el administrador (admin).

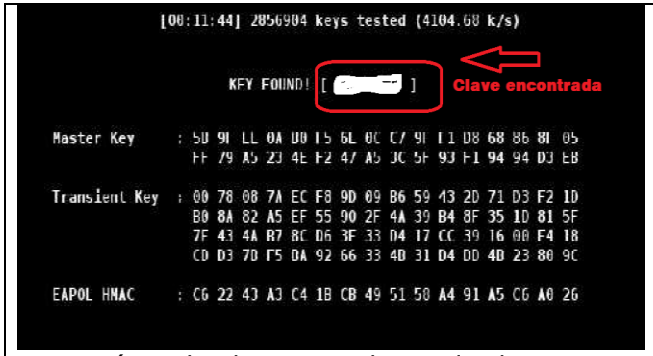
Pasamos a otro comando para tratar de burlar el sistema con el usuario:

Utilizamos un diccionario extenso pero el resultado de fuerza bruta dio negativo, esto se debe a una contraseña de admin fuerte, esta recomendación debe persistir.		
6. Ingeniería social aplicada a docentes para obtener contraseñas de SIGEDIN. Se creó un protocolo para llamar a algunos docentes seleccionados al azar, unos de primaria y otros de bachillerato cuyos nombres no se revelan para evitar problemas laborales y discusiones. Siguiendo el protocolo se logró conseguir la contraseña de acceso al sistema de evaluación SIGEDIN de dos (2) profesores de diez (10). 1. Se consigue el número de celular en Secretaria del docente y se lo llama en horario de trabajo para evitar más atención. 2. Se hace pasar por funcionario de	Servicios Febrero 21/2015 Jairo Quintero	Crear un sistema de capacitación y concientización de seguridad dirigida a todos los usuarios.

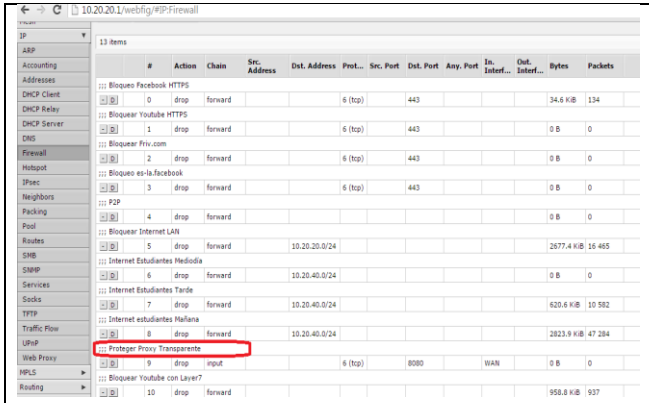
Xolumatica, empresa encargada de crear el software de la ciudad de Mocoa. 3. Solicita que necesitan entrar a su cuenta porque ha sido detectado un problema y necesita ser reparado de inmediato en Sigedin. 4. Por ende, se pide la contraseña de acceso para solucionar el problema y reiniciar a la normalidad. 5. Fin de la conversación. 6. Los datos son entregados únicamente al Ing. Jairo Quintero sin revelar nombres.		
7. Criptografía aplicada a las conexiones web. Se verificó que no hay ninguna conexión SSL, por lo tanto es posible escuchar o intervenir la comunicación para detectar el logueo y tratar de sacar una clave, sobre todo desde el interior de la	Servicios Febrero 21/2015 Jairo Quintero	Implementar el protocolo SSL en el Hosting, para las conexiones más relevantes como el sistema SIGEDIN y evitar ataques de “escucha” entre otros, así mismo el cambio de Hash de MD5 a SHA 256 que es más seguro.

red de la institución.  Sistema de evaluación SIGEDIN.  La base de datos “SIGEDIN” en Mysql tiene Hash MD5 que aunque es vulnerable se necesita una colisión y un ataque de fuerza bruta y de contraseñas débiles para poderlo vulnerar, caso que sería lejano en posibilidades pero que podría		

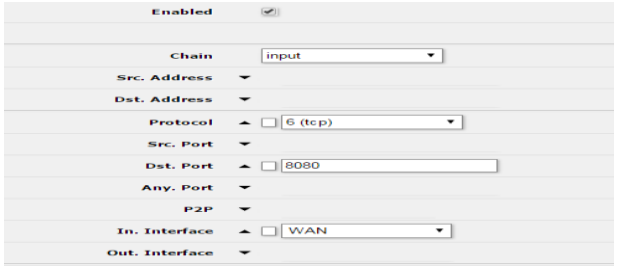
ocurrir.		
8. Vulnerabilidades de la red Wifi tanto docentes como estudiantes. Funcionan con NanoStation M2 y M5 para interconectar las dos sedes, también una antena Mikrotik Metalica, todas tienen configurado seguridad WPA2 con contraseñas normales, es decir, sin respetar las reglas de contraseñas seguras o fuertes, la unión de un dispositivo con otro se hace teniendo en cuenta el filtro MAC. Se hizo un hackeo ético con la respectiva autorización a una de las contraseñas débiles, encontramos un resultado positivo donde se pudo descifrar la clave en corto tiempo, utilizando el programa Wifislax y creamos una red de prueba utilizando la misma contraseña real.	Red Febrero 22/2015 Jairo Quintero	Crear contraseñas fuertes para WPA2 en cada antena o dispositivo, igualmente desactivar en todos WPS para evitar otros ataques.

 No costó mucho tiempo en obtener la clave que no es revelada en este documento pero que demuestra una mala configuración de la misma. Para el caso de los demás dispositivos que tienen contraseña más fuerte no fue posible encontrarla, incluso ni utilizando diccionarios de fuerza bruta más extensos y variados.		
9. Vulnerabilidades de la red alámbrica La red cableada ocupa solo una parte de la institución, une las dos salas de cómputo con la red central y los dos servidores, en algunas partes no cuenta con canaletas que cubran y ayuden a	Red Febrero 23/2015 Jairo Quintero	Instalar canaletas metálicas para los cables externos. Restringir el acceso físico a los dispositivos y servidores, controlar el acceso lógico.

evitar daños o deterioro del cable, así mismo que alguien pueda extraer un cable y conectar algún dispositivo por medio cableado. El acceso físico a los dispositivos y servidores no es restringido ni controlado.		
10. Análisis de las reglas del proxy y Firewall y protección del mismo. Las reglas del proxy están configuradas en un Mikrotik RB750, generalmente son para bloqueos de páginas y control de navegación, pero hay una regla para evitar que ataquen el puerto 8080 del proxy cache.	Red Febrero 24/2015 Jairo Quintero	Se deben cerrar los puertos no utilizados como el 23 de telnet, 21 de ftp para evitar ataques. Crear otras reglas en el firewall para proteger más la red.



Esta es la configuración:



Análisis de la configuración Proxy:

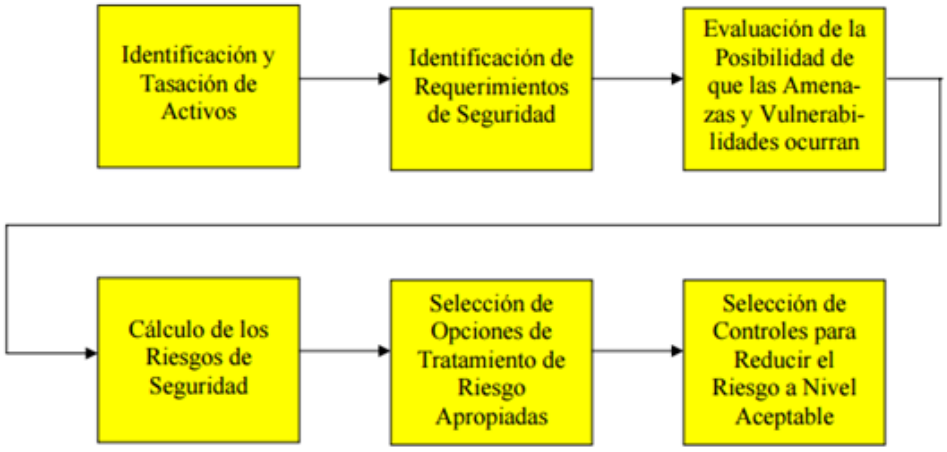
11 items | | # | Src. Address | Dst. Address | Dst. Port | Dst. Host | Path | Method | Action | Redirect To | Hits | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | ;;; Bloquear Youtube normal | | | | | | | | | | | | - D | 0 | | | | *.youtube.com* | | | deny | www.google.com.co | 849 | | ;;; Bloquear Facebook normal | | | | | | | | | | | | - D | 1 | | | | *.facebook.com* | | | deny | www.google.com.co | 225 | | ;;; SEXO | | | | | | | | | | | | - D | 2 | | | | *.sexo* | *.sexo* | | deny | | 0 | | ;;; Bloquear Friv | | | | | | | | | | | | - D | 3 | | | | *friv* | | | deny | | 41 | | - D | 4 | | | | | *.zip* | | deny | | 23 | | - D | 5 | | | | | *.rar* | | deny | | 0 | | - D | 6 | | | | | *.exe* | | deny | | 564 | | - D | 7 | | | | | *.mp3* | | deny | | 12 | | - D | 8 | | | | | *.mp4* | | deny | | 14 | | - D | 9 | | | | | *.avi* | | deny | | 0 | | - D | 10 | | | | | *.flv* | | deny | | 0 | Estas reglas están encaminadas a controlar navegación, no hay reglas para cerrar puertos abiertos libres. Al verificar sus puertos se pudo constatar que tiene algunas vulnerabilidades, sobre todo con el puerto 23 para telnet que generalmente se usa para atacar servidores y dispositivos por no estar encriptado.		

Fuente: Autor

9. PROCESO DE EVALUACIÓN Y ANÁLISIS DEL RIESGO

El proceso de evaluación del riesgo se plasma en el siguiente gráfico, donde se orientan las fases usadas para este componente.

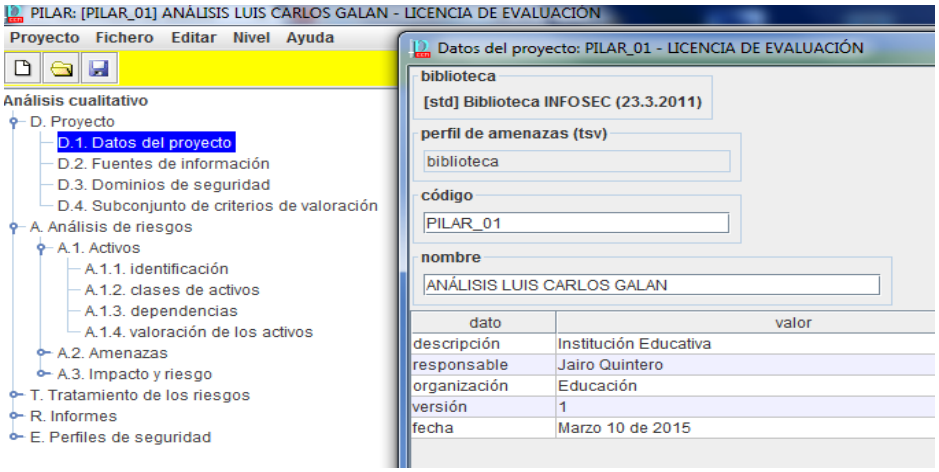
Figura 4. Proceso de evaluación del riesgo



Fuente:
http://www.iso27000.es/download/Analisis_del_Riesgo_y_el_ISO_27001_2005.pdf

Para este análisis de riesgos sobre los activos identificados, se utilizó la herramienta PILAR versión 5.1 que utiliza la metodología Magerit Versions 3.

Figura 5 Proyecto de Activos y riesgos en Software Pilar



Fuente: Autor

9.1 LISTA DE ACTIVOS

Por medio de Magerit se valora cada activo asignando a través de una escala de 0 a 10 la confidencialidad, integridad, autenticidad, disponibilidad y trazabilidad de estos, donde 0 toma valor de irrelevante y 10 daño muy grave para la institución.

Se pueden observar todos los activos informáticos de la institución según la metodología seleccionada, a través de la siguiente tabla.

Tabla 2. Lista de activos

ID	Activo	Tipo de Activo
	Firewall y proxy Interno	Hardware
2	Punto de acceso Wifi	Hardware
3	Servidores para Moodle y Latin Campus	Hardware
4	Equipos de Usuarios	Hardware
5	Punto de acceso punto a punto	Hardware
6	Software servidores Moodle y Latin Campus	Software
7	Windows 7 Profesional	Software
8	Software SIGEDIN	Software
9	Routers	Red
10	Switches LAN	Red
11	Información contenida en servidores Moodle y Latin Campus	Información
12	Información contenida en Software SIGEDIN	Información
13	Secretaria general y operadora del sistema Sigedin	Personal
14	Ingeniero Administrador de red y servicios.	Personal
15	Cableado de Datos y eléctrico	Instalación

Fuente: Autor

9.2 EVALUACIÓN DE ACTIVOS

Siguiendo la metodología Magerit se procede a evaluar los activos, la herramienta ayuda a evaluar los mismos y luego con la identificación de las amenazas, se utiliza PILAR, que ayuda también a la identificación de riesgos.

Tabla 3. Evaluación de activos

TIPO	ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	AUTENTICIDAD	TRAZABILIDAD
Hardware	Servidores	8	7	9	6	9
Red	Router	5	3	3	2	1
Información	Contenido de servidores y Sigedin	9	8	8	8	8
Red	Switch	9	4	4	5	5
Hardware	Firewall	9	4	4	5	5
Hardware	Estaciones de trabajo	6	3	4	4	5
Personal	Empleados	7	5	6	5	4
Software	Conjunt	7	9	9	9	9

	o de programas					
Servicio	Punto a punto - aire	1	1	1	1	1

Fuente: Autor

10. EVALUACIÓN DE RIESGOS

Se desarrollan tres (3) procesos para el presente proyecto.

10.1 PLANIFICACIÓN

Es importante porque se constituye en el marco de referencia del proyecto.

10.2 ESTUDIO DE OPORTUNIDAD

Tiene como objetivo específico, realizar un diagnóstico del estado actual de seguridad en que se encuentran los activos de información y los tecnológicos dentro de la Institución Educativa Luis Carlos Galán, además de motivar a la dirección institucional para implementar el SGSI.

10.3 DEFINICIÓN DEL ALCANCE Y OBJETIVOS DEL PROYECTO

Después de contar con el aval para la realización del proyecto para la creación e implementación del SGSI en la Institución Educativa Luis Carlos Galán, se definen los límites y objetivos del trabajo para alcanzar el éxito.

Los objetivos han sido planteados con el propósito de realizar un concienzudo y real análisis de riesgos que lleven a una futura implementación del sistema de gestión de seguridad de la información de la I.E. LUIS CARLOS GALAN.

10.4 PLANIFICACIÓN DEL PROYECTO

Es necesario crear un cronograma de actividades que definan el alcance y el tiempo y ejecución de la implementación del SGSI.

10.5 LANZAMIENTO DEL PROYECTO

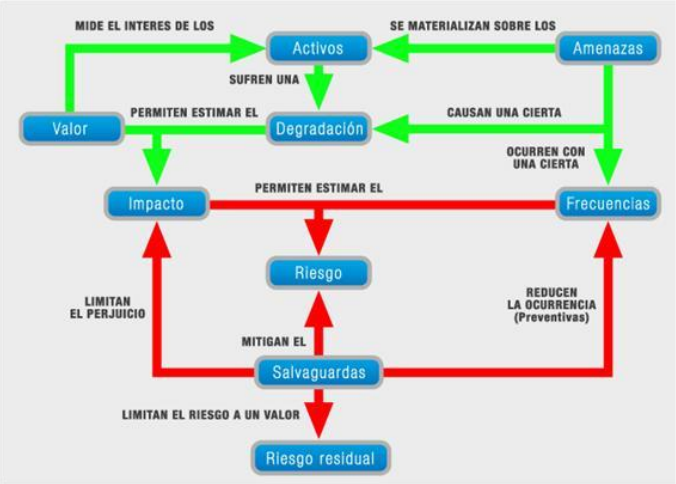
Con la autorización del consejo directivo y rector de la institución, se inicia el proceso de análisis de riesgos, se procede con la técnica de observación directa,

análisis de lo existente y entrevista para la recolección de la información siendo estas las más apropiadas, se tiene la ventaja de que el autor de este proyecto es el mismo administrador de la red y servicios informáticos de la institución, por lo tanto estamos directamente involucrados con la misma información.

11. ANÁLISIS DE RIESGOS

Según la herramienta PILAR de Magerit, estos tienen un comportamiento que se describen en el siguiente gráfico.

Figura 5. Análisis de riesgos según Pilar



Fuente: https://seguridadinformaticaufps.wikispaces.com/

Como toda empresa o institución educativa como este caso, tiene diferentes riesgos los cuales pueden convertirse en un momento dado en vulnerabilidades, por tal razón es importante a través de Magerit valorar y clasificar los activos de forma correcta y dándole la importancia para sacar adelante los objetivos del proyecto.

11.1 CARACTERIZACIÓN Y VALORACIÓN DE LOS ACTIVOS

Abarca las siguientes tareas:

11.1.1 Identificación de los activos según Magerit. Ahora se clasifican como en uno de los puntos anteriores, pero teniendo en cuenta el Libro II de la Metodología Magerit 3, con el catálogo de elementos según el Anexo A en el punto 2:

Tabla 4. Clasificación de activos

TIPO	NOMBRE DEL ACTIVO
APLICACIONES INFORMATICAS	1. [SI_SIGEDIN] Sistema de Gestión Académica. 2. [SI_Moodle] Plataforma Virtual. 3. [SI_Latin Campus] Plataforma Virtual Inglés. 4. [SO] Sistema Operativo. 5. [HER_SW] Herramientas Software. 6. [ANT_VIR] Anti virus
SERVICIOS	7. [S_DHCP] Servidor DHCP 8. [S_PAGINA WEB] Página web en servicio de hospedaje Hosting privado. 9. [S_PER_VIRTUAL] Periódico virtual y Blogs.
REDES DE COMUNICACIONES	10. [RO_LAN] Router 11. [RO_LAN]Switche
EQUIPAMIENTO INFORMATICO	12. [FW_MIKROTIK] Firewall / Equipo Unificado contra Amenazas y administración de la red. 13. [PC] Equipos de computo 14. [SW_A] Switch Administrable
EQUIPAMIENTO AUXILIAR	15. [CAB_RED] Cableado de Red
PERSONAL	16. [AS_ADOR] Administrador red y servicios.

Fuente: Autor

11.1.2 Valoración de Activos. Según la metodología MAGERIT Versión 3; se usan las siguientes dimensiones[3]:

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de la Información.
- [A] Autenticidad
- [T] trazabilidad

Tabla 5. Escala de valoración de activos

VALOR			CRITERIO
10	Extremo	E	Daño extremadamente grave.
9	Muy alto	MA	Daño muy grave
6-8	Alto	A	Daño grave
3-5	Medio	M	Daño importante
1-2	Bajo	B	Daño menor
0	Despreciable	D	Irrelevante a efectos prácticos

Fuente: Metodología Magerit, Libro II.

Se procede según la metodología a valorar los activos según el tipo que corresponda de los obtenidos en la institución educativa.

[3] Tomado de: 2012_Magerit V3, libro2, catálogo de elementos, página 19.

11.1.3 Valoración de Activos tipo Aplicaciones

Tabla 6. Valoración de activos tipo aplicaciones

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[SI_SIGEDIN] Sistema de Información Académica**(1)**.	[MA]	MA]	[MA]	[A]	[A]
[SI_Moodle] Herramientas virtuales de aprendizaje. **(2)**	[MA]	[A]	[A]	[A]	
[SI_Latin Campus] Plataforma virtual de Inglés**(3)**.	[MA]	[A]	[A]	[A]	
[SO]Sistema Operativo**(4)**.	[MA]	[A]			
[HER_SW] Herramientas Software**(5)**	[MA]	[A]			
[ANT_VIR] Antivirus**(6)**	[A]				

Fuente: Autor

(1) [4.pi1] probablemente afecte a un grupo de individuos

[5.lro] probablemente sea causa de incumplimiento de una ley o regulación **[9.si]** probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios

[1.po] pudiera causar protestas puntuales.

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

[1.lg] Pudiera causar una pérdida menor de la confianza dentro de la organización

(2) [4.pi1] probablemente afecte a un grupo de individuos

[7.lro] probablemente cause un incumplimiento grave de una ley o regulación **[10.si]** probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios **[5.da2]** Probablemente cause un cierto impacto en otras organizaciones **[5.olm]** Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local

[2.lg] Probablemente cause una pérdida menor de la confianza dentro de la Organización

[4.crm] Dificulte la investigación o facilite la comisión de delitos

[8.lbl] Confidencial

(3) [4.pi1] probablemente afecte a un grupo de individuos

[3.si] probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente

[7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones

[3.po] causa de protestas puntuales

[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

[1.adm] Pudiera impedir la operación efectiva de una parte de la Organización

[7.rto] RTO < 4 horas

(4) [6.pi2] probablemente quebrante seriamente la ley o algún reglamento de protección de información personal

[7.lro] probablemente cause un incumplimiento grave de una ley o regulación
[3.si] probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente

[3.da] Probablemente cause la interrupción de actividades propias de la Organización

[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(5) [6.pi2] probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.

[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[3.si] Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente

[3.da] Probablemente cause la interrupción de actividades propias de la Organización

[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

11.1.4 Valoración de Activos Tipo Servicios

Tabla 7. Valoración de activos tipo servicios

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[S_DHCP] Servidor DHCP**(7)**		[MA]	[A]		
[S_PAGINA WEB] Página web en servicio de hospedaje Hosting privado.. **(8)**	[E]	[A]	[A]		
[S_PER_VIRTUAL] Periódico virtual y Blogs **(9)**	[E]	[A]	[A]		

(7) [6. pi2] probablemente quebrante seriamente la ley o algún reglamento de protección de información personal

[7.lro] probablemente cause un incumplimiento grave de una ley o regulación **[1.si]** pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

[5.olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local

(8) [6.pi1] probablemente afecte gravemente a un grupo de individuos

[9.si] probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios

[9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones

[6.po] probablemente cause manifestaciones, o presiones significativas

[3.adm] probablemente impediría la operación efectiva de una parte de la Organización

(9) [1.pi1] pudiera causar molestias a un individuo

[3.si] probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente

[9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones

[6.po] probablemente cause manifestaciones, o presiones significativas

[3.adm] probablemente impediría la operación efectiva de una parte de la Organización

11.1.5 Valoración de Activos Tipo Redes de Comunicaciones

Tabla 8. Valoración de activos tipo redes de comunicaciones.

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[RO_LAN] Router **(10)**	[MA]	[A]			
[RO_LAN]Switche **(11)**	[MA]	[A]			

Fuente: Autor

(10) [5.pi2] probablemente quebrante seriamente leyes o regulaciones

[9.lro] probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación

[10.si] probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios

[9.cei.e] constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros

[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística

[5.lg.b] Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público

(11) [5.pi2] probablemente quebrante seriamente leyes o regulaciones

[9.lro] probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación

[10.si] probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios

[9.cei.e] constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros

[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística

11.1.6 Valoración de Activos Tipo Equipamiento informático

Tabla 9. Valoración de activos tipo equipamiento informático.

Activo	Dimensiones de				
	[D]	[I]	[C]	[A]	[T]
[FW_MIKROTIK] Firewall / Equipo Unificado contra Amenazas y administración de la red**(12)**.	[MA]	[A]			
[PC] Equipos de cómputo**(13)**	[MA]	[A]			
[SW_A] Switch Administrable**(14)**	[MA]	[A]			

Fuente: Autor

(12) [6.pi2] probablemente quebrante seriamente la ley o algún reglamento de protección de información personal

[7.lro] probablemente cause un incumplimiento grave de una ley o regulación

[10.si] probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios

[9.cei.e] constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros

[9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones

[6.po] probablemente cause manifestaciones, o presiones significativas **[7.olm]**

Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

[2.lg] Probablemente cause una pérdida menor de la confianza dentro de la Organización

(13) [5.pi1] probablemente afecte gravemente a un individuo

[3.lro] probablemente sea causa de incumplimiento leve o técnico de una ley o regulación

[7.si] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves

[7.cei.d] proporciona ganancias o ventajas desmedidas a individuos u organizaciones

[5.da] Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones

[1.po] pudiera causar protestas Puntuales

[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(14) [5.pi1] probablemente afecte gravemente a un individuo

[3.lro] probablemente sea causa de incumplimiento leve o técnico de una ley o regulación

[7.si] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves

[7.cei.d] proporciona ganancias o ventajas desmedidas a individuos u

organizaciones

[7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones

[6.po] probablemente cause manifestaciones, o presiones significativas **[9.olm]** Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística

[5.lg.b] Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público

11.1.7 Valoración de Activos Tipo Equipamiento Auxiliar

Tabla 10. Valoración de activos tipo equipamiento auxiliar.

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[CAB_RED] Cableado de Red **(15)**	[MA]	[A]			

Fuente: Autor

(15) [4.pi1] probablemente afecte a un grupo de individuos

[3.si] probablemente sea causa de una disminución en la seguridad o dificulte la investigación de un incidente

[7.cei.d] proporciona ganancias o ventajas desmedidas a individuos u organizaciones

[7.da] probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones

[6.po] probablemente cause manifestaciones, o presiones significativas [7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

[7.adm] probablemente impediría la operación efectiva de la Organización

11.1.8 Valoración de activos Tipo Personal

Tabla 11. Valoración de activos tipo personal

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[AS_ADOR] Administrador red y servicios **(16)**	[MA]	[A]			

(20) [6.pi1] probablemente afecte gravemente a un grupo de individuos

[7.si] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves

[3.cei.d] facilita ventajas desproporcionadas a individuos u organizaciones.

[7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.

[5.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.

[6.po] probablemente cause manifestaciones, o presiones significativas

[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.

[5.adm] probablemente impediría la operación efectiva de más de una parte de la Organización.

[7.lg.b] Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general.

11.2 CARACTERIZACIÓN Y VALORACIÓN DE LAS AMENAZAS

Consiste en determinar la degradación del activo; proceso que consiste en evaluar el valor que pierde el activo (en porcentaje) en caso que se efectúe una amenaza.

Estas Amenazas se han tomado del catálogo de elementos que presenta la metodología MAGERIT en su libro II Versión 3.0

A continuación se expresan los rangos según la frecuencia de degradación con que se manifiesten así:

Tabla 12. Frecuencia de amenazas.

Valor			Criterio
4	Muy frecuente	MF	A diario
3	Frecuente	F	Mensualmente
2	Normal	FN	Una vez al año
1	Poco frecuente	PF	Cada varios años

Fuente: Magerit V.3 - Libro II - Catálogo de Elementos

11.2.1 Degradación de las Amenazas

Tabla 13. Valor degradación de amenazas

Valor	Criterio	
100%	MA	Degradación MUY ALTA del activo
80%	A	Degradación ALTA considerable del activo
50%	M	Degradación MEDIANA del Activo
10%	B	Degradación BAJA del Activo

Fuente: Magerit V.3 - Libro II - Catálogo de Elementos

11.2.2 Identificación y Valoración de Amenazas Tipo Aplicaciones Informáticas

Tabla 14. Valor degradación de amenazas aplicaciones informáticas

Activo / Amenaza	Frecuencia	Dimensiones de				
		D	I	C	A	T
[E.1] Errores de los Usuarios	F	MA	A			
[E.2] Errores del administrador	FN	A				
[E.4] Errores de Configuración	FN	A				
[E.14] Escapes de Información	PF			A		
[E.18] Destrucción de información	PF	MA		A		
[A.11] Acceso no Autorizado	FN	MA				
[A.15] Modificación de la Información	PF		MA			

Fuente: Autor

11.2.3 Justificación de Amenazas Aplicaciones Informáticas

[E.1] Errores de los usuarios: Se considera que este tipo de amenaza llegue a presentarse frecuentemente debido a que los usuarios o personal nuevo no es capacitado(a) adecuadamente en el uso de activos "aplicaciones informáticas", esto puede afectar de una u otra manera ya que estos activos están relacionados con los objetivos de la institución educativa y su modelo de negocio, en casi de llevarse a cabo una amenaza puede generar una paralización de un gran porcentaje en el funcionamiento normal de la institución.

[E.2] errores del administrador: Se da un valor ALTO, pero en si es poco frecuente que se genere este tipo de situación dado el nivel del administrador y su experiencia.

[E.4] Errores de configuración: Se valora como de ALTA degradación porque debido a una mala configuración en los activos pertenecientes a las aplicaciones informáticas llevaría a ataques como intrusión, denegación de servicios, robo de información, etc. Afectando directamente el corazón informático de la Institución Educativa Luis Carlos Galán, llevándola a una suspensión de los servicios ofrecidos.

[E.14] Escapes de información: Se considera que la afectación sería Alta para la dimensión de Confidencialidad, ya que si hay escape de información esta puede ser modificada o usada para beneficios propios llevando a pérdida de confianza Institucional.

[E.18] Destrucción de información: Dado el caso de llegarse a presentar esta amenaza las dimensiones más afectadas son la Disponibilidad y la Confidencialidad, porque los activos de las aplicaciones informáticas guardan toda la información que se maneja a diario dentro de los procesos de gestión académica de la Institución.

[A.11] Acceso no autorizado. La dimensión que afecta directamente es la Disponibilidad y se considera muy alta porque al presentarse una intrusión desencadenaría la materialización de las amenazas [E.14], [E.18] y [A.15] entre otras, dejando en grave riesgo la información en general como activo más importante.

[A.15] Modificación de la información: Afectará directamente la dimensión de integridad en un nivel muy alto, porque de presentarse ataques de modificación de información se van a ver alterados los datos almacenados en los activos pertenecientes a este grupo, causando un caos informático y arrojando datos erróneos a la hora de las consultas y transacciones en cada uno de los procesos normalizados dentro de las labores institucionales.

11.2.4 Identificación y Valoración de Amenazas Tipo Servicios

Tabla 15. Valor degradación de amenazas servicios

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

Fuente: Autor

11.2.5 Justificación de Amenazas Servicios

[E.20] Vulnerabilidades de los programas: La probabilidad de ocurrencia se

consideró como PF y que afectará directamente la disponibilidad porque los programas usados para dar soporte a los servicios implementados en la Institución han sido probados con anterioridad por la misma empresa proveedora del software y por otras instituciones como tal.

[A.5] Suplantación de la identidad del usuario: Este es quizá una de las mayores amenazas visibles dentro de los servicios que ofrece la Institución debido a que no se han implementado normativas para el uso de contraseñas fuertes y los docentes y estudiantes no tienen el conocimiento ni la experiencia para saber cuándo crear una contraseña de este tipo, pudiéndose efectuar ataques para robar o conseguir sus claves a través de diferentes métodos.

[A.8] Difusión de Software dañino: Esta amenaza es considerada de alto grado de degradación y que pudiese presentar en un nivel de frecuencia normal; con afectación directa a la disponibilidad; debido a la gran cantidad de equipos de cómputo que están destinados para los alumnos y por la falta de concientización que hay sobre el uso de software licenciado y descarga de archivos que no redundan en la educación, sobre todo en el intercambio entre estudiantes.

[A.24] Denegación de Servicio, Se ha valorado de muy alta degradación en la dimensión de disponibilidad, porque se pueden llegar a presentar errores de programación que no permiten a usuarios autorizados acceder al sistema. Esta amenaza puede ser causa de una reacción en cadena con otras amenazas; pero con poca frecuencia de ocurrencia dado las pruebas efectuadas con anticipación al software utilizado.

11.2.6 Identificación y Valoración de Amenazas Tipo Redes de Comunicaciones

Tabla 16. Valor degradación de amenazas redes de comunicaciones

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[N.*] Desastres Naturales		MA				MA
[I.5] Avería de origen físico o lógico	PN	MA				
[I.8] Fallo de Servicio de Comunicaciones	PF	A				
[E.2] Errores del Administrador	PF	A		A		
[A.4] Manipulación de Configuración.	PF			A	A	

Fuente: Autor

11.2.7 Justificación de Amenazas Redes de Comunicaciones

[N.*] Desastres Naturales: Se puede llegar a presentar y la disponibilidad de los activos de redes de comunicaciones tendría un detrimento muy alto porque se caerían todos los servicios llevando a una paralización total de las actividades en los procesos.

[I.5] Avería de origen físico o lógico: Las instalaciones no son muy adecuadas y una falla de este tipo puede llegar a afectar todo el funcionamiento normal de todos los sistemas instalados.

[I.8] Fallo de Servicio de comunicaciones: Actualmente solo se cuenta con un proveedor de internet subsidiado a través del Ministerio de Educación Nacional, su afectación genera problemas en las comunicaciones desde la institución hacia afuera, sobre todo los sistemas en línea que actualmente tiene.

[E.2] Errores del administrador: Por errores del administrador se puede llegar a tener un Alto grado de degradación en las dimensiones de disponibilidad y confidencialidad ya que al no ser un dispositivo propio la administración está en manos de la Empresa prestadora de este servicio.

[A.4] Manipulación de Configuración: Este ítem está ligado directamente con el numeral y las razones expuestas en el numeral anterior.

11.2.8 Identificación y Valoración de Amenazas Tipo Equipamiento Informático

Tabla 17. Valor degradación de amenazas Equipamiento informático

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

Fuente: Autor

11.2.9 Justificación de Amenazas Equipamiento Informático

[N.1] Fuego: Se consideró de muy alto impacto en todas las dimensiones

(disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) al llegarse a presentar fuego como desastre natural porque se perdería todo el equipamiento informático que es el soporte de los demás activos de información como los relacionados en aplicaciones informáticas, servicios, redes de comunicaciones. No se tiene una protección contra esta amenaza, debido a que la institución ha ido adquiriendo estos activos de acuerdo a las necesidades sin ningún tipo de planeación y control directo, no tiene equipos de protección contra incendios ni alarmas.

[I.2] Daños por Agua. La degradación se consideró como alta en disponibilidad y de poca frecuencia porque, en la región llueve bastante y es un terreno húmedo, situación que atrae el problema aunque no es frecuente, además los sitios donde se encuentran no están bien diseñados para evitar un daño de este tipo.

[I.5] Avería de origen físico o lógico: En nivel de degradación que puede presentarse en cuanto a averías de origen físico o lógico son altas afectando la destinadas como centros de datos, se usan además como zonas de almacenamiento de equipos de cómputo obsoletos, otra razón es que la mayoría de equipamiento informático está sometido a largas jornadas de uso (salas de cómputo y laboratorios) con lo que se pueden presentar fallas de físicas o de desconfiguración sin un control adecuado.

[E.23] Errores de mantenimiento/ actualización de equipos (hardware): El mantenimiento está a cargo de un docente, lo que hace más difícil tener al día todos los equipos tanto en software como en hardware, esto también puede traer problemas como errores de este tipo ya que la institución educativa no cuenta con recursos para contratar personal extra.

[A.11] Acceso no Autorizado: La confidencialidad para este ítem dentro del equipamiento informático es alto porque no existen controles físicos ni lógicos

para el ingreso de personal no autorizado a ciertas áreas.

[A.23] Manipulación de los equipos. Se considera que el grado de degradación que se puede llegar a experimentar es alto en la dimensión de confidencialidad especialmente en los equipos de cómputo de la parte administrativa porque no se han tomado medidas o políticas de seguridad que concienticen a los usuarios en el uso exclusivo del personal contratado en la Institución y del uso de nombre de usuario y contraseña fuerte, y el bloqueo de los equipos en ausencia de estos.

11.2.10 Identificación y Valoración de Amenazas Tipo Equipamiento Auxiliar

Tabla 18. Valor degradación de amenazas Equipamiento auxiliar

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

Fuente: Autor

11.2.11 Justificación De Amenazas Equipamiento Auxiliar

[I.5] Avería de origen físico o lógico: No hay protección de los equipos físicos y esto puede traer algunos problemas de disponibilidad ante una falla, también no existen dispositivos adecuados de protección eléctrica ni de UPS.

11.2.12 Identificación y Valoración de Amenazas Tipo Personal

Tabla 19. Valor degradación de amenazas personal

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

Fuente: Autor

11.2.13 Justificación De Amenazas Personal. [E.7] Deficiencia en la organización. Se valora como frecuencia normal y de degradación de disponibilidad como Alta porque la institución Educativa Luis Carlos Galán por ser pública y no contar con recursos propios suficientes, solo los que gira el gobierno nacional anualmente, se es insuficiente el personal tanto de seguridad como de sistemas, situación que trae problemas de amenazas en cuanto a la prevención que se debe tener en los activos.

[E.15] Alteración accidental de la información: Por haber poco personal directo encargado no solo de la parte de seguridad y administración, sino de otras labores como digitación de estudiantes nuevos al inicio de cada año, puede darse el caso de que un digitador(a) pueda efectuar daños en la información, sobre todo al no existir cuentas de usuario en el sistema Sigedin con roles mejor distribuidos.

[A.30] Ingeniería Social: Es uno de los problemas que mayor auge tiene actualmente no solo en la humanidad sino en esta institución, pues el personal de usuarios no está capacitado para enfrentar problemas de esta índole, según se

pudo dar cuenta en un estudio realizado dentro de la misma institución y el cual se puede observar anexo al presente documento, por lo tanto afecta a la Confidencialidad de la información y es frecuente.

12. SALVAGUARDAS

12.1 CARACTERIZACIÓN DE LAS SALVAGUARDAS

Esta se realiza de acuerdo al nivel de criticidad de los activos incluidos en el análisis de riesgos de la institución Educativa Luis Carlos Galán contemplados en el presente documento, basados en el catálogo de elementos que proporciona Magerit.

12.1.1 Salvaguardas Activos Protecciones Generales u Horizontales

Tabla 20. Salvaguardas protecciones generales u horizontales

SALVAGUARDAS	DIMENSIÓN	EVALUACIÓN
Control de acceso lógico	[A], [D], [C]	30%
Gestión de incidencias	[D], [C], [T], [A], [I]	50%

Fuente: Autor

12.1.2 Descripción de Salvaguardas. **Control de acceso lógico:** Existen medidas básicas para al acceso a las aplicaciones y servicios web a través de la autenticación de usuarios, si bien existen formas de control de acceso, estos son muy básicos y es necesario implementarlos mejor para prevenir riesgos.

Gestión de incidencias: No existe un sistema de control de incidencias para algunos sistemas importantes como Sigedin, además no se hace seguimiento a las mismas ni tampoco existe un sistema de control o auditoria interna de la base de datos para hace seguimiento de los ingresos de los usuarios.

12.1.3 Salvaguardas Activos Protección De Los Datos/Información

Tabla 21. Salvaguardas protecciones de los datos e información

SALVAGUARDAS	DIMENSIÓN	EVALUACIÓN
Copias de Seguridad de los Datos (Backup)	[I], [A], [C], [D], [T]	5%
Cifrado de la información	[C], [T], [A], [I]	50%

Fuente: Autor

12.1.4 Descripción de las salvaguardas. **Copias de Seguridad de los Datos:** Todos los sistemas y servidores de la institución cuentan con un sistema de backup automático el cual se guarda dentro del mismo sistema o servidor, pero ante el caso de una falla en los discos de almacenamiento pueden haber problemas serios de pérdida de información, como también ante un eventual caso de ataque al sistema operativo o daño del mismo; para este caso se propone adquirir un dispositivo NAS instalado directamente a la red local para crear copias en discos duros externos de forma automática programada, sin abandonar las copias internas.

Cifrado de información: Especialmente para los servicios en línea a través de internet como el sistema “Sigedin” es necesario implementar el cifrado mediante los protocolos SSL-TSL, con el fin de evitar ataques, sobre todo cuando se accede desde la red local o Wifi que es donde se pueden hacer ataques a los equipos conectados, como también para accesos desde equipos fuera de la institución que generalmente tienen virus o malware.

12.1.5 Salvaguardas Activos Protección De Los Servicios

Tabla 22. Salvaguardas protecciones de los servicios

SALVAGUARDAS	DIMENSIÓN	EVALUACIÓN
Se aplican perfiles de seguridad	[A], [I], [D]	50%
Protección de servicios y aplicaciones web	[I],[D]	40%

Fuente autor

12.1.6 Descripción Salvaguardas. **Se aplican perfiles de seguridad:** Estos perfiles se aplican desde el firewall y el proxy interno, en los servidores no existen perfiles suficientes como la activación del firewall interno que cada sistema operativo para servidores tiene y no se cuenta con software antivirus para todos los equipos, igualmente software antimalware o antispyware, por lo tanto se deben adquirir paquetes de licencias de estos programas para todos los computadores de la institución.

Protección de servicios y aplicaciones web: La protección web únicamente se hace a través de las políticas y herramientas del servidor Hosting donde se paga dicho alojamiento, es necesario crear políticas para el manejo y autenticación en los mismos.

12.1.7 Salvaguardas Activos Protección De Las Aplicaciones (Software)

Tabla 23. Salvaguardas protección de las aplicaciones

Salvaguardas	Dimensión	Evaluación
Cambios (Actualizaciones y mantenimiento)	[I],[D], [T]	80%

Fuente: Autor

12.1.8 Descripción de salvaguardas. **Cambios (Actualizaciones y mantenimiento):** Se deben crear políticas para actualizaciones a través de cambios propuestos cada año para mejorar el mismo, estos cambios se deben efectuar en horarios que no afecten el normal funcionamiento de la institución.

12.1.9 Salvaguardas Activos Protección De Los Equipos (Hardware)

Tabla 24. Salvaguardas protección de las aplicaciones

Salvaguardas	Dimensión	Evaluación
Operación	[D]	60%
Cambios (Actualizaciones y mantenimiento)	[D], [T]	70%

Fuente: Autor

12.1.10 Descripción de salvaguardas. **Operación:** La manipulación de los equipos no se hace de acuerdo a unas políticas creadas ni de helpdesk, en las salas de cómputo no hay carteles alusivos al tema.

Cambios (Actualizaciones y mantenimiento): No se hace de acuerdo a una programación unificada, solo cuando hay reportes o averías, sin tener en cuenta normas de calidad, eficiencia y organización.

12.1.11 Salvaguardas Activos Protección De Las Comunicaciones

Tabla 25. Salvaguardas protección de las aplicaciones

Salvaguardas	Dimensión	Evaluación
Internet: Uso de? Acceso a	[D], [C],[T]	90%
Seguridad Wireless (WiFi)	[D], [C]	50%

Fuente: Autor

12.1.12 Descripción de salvaguardas. **Internet: Uso de? Acceso a:** Se aplican y monitorean perfiles para asegurar el acceso a internet a través del firewall y proxy interno, no solo en el perfil de seguridad aplicado se evalúan y restringen los accesos a sitios específicos o se aplican técnicas de webfiltering, también se gestiona tráfico y disponibilidad de ancho de banda, escaneo de posibles virus y capacidad de descarga en cuanto a un límite de tamaño por archivo. Se relacionan las dimensiones de Disponibilidad, Confidencialidad y Trazabilidad. La evaluación en general del salvaguarda se mantiene constante y en buenos criterios de efectividad.

Seguridad Wireless (WiFi): Se tiene la red inalámbrica separada física y lógicamente del resto de la red institucional, hay control en los protocolos de salida y entrada, se aplica control en ancho de banda y control de uso de aplicaciones p2p en conjunto con webfiltering y escaneo de virus y spam de salida, control de acceso entre usuarios o aislamiento AP.

13. RIESGOS

13.1 ESTIMACIÓN DEL ESTADO DE RIESGO

Esta actividad se realiza con el propósito de analizar los datos recopilados en las actividades anteriores y evaluar el estado de riesgo, donde se incluye la estimación de impacto y riesgo. Se toma la siguiente escala para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo:

Tabla 26. Escala de calificación de activos

	MA: muy alto
	A: alto
	M: medio
	B: bajo
	MB: muy bajo

13.2 ESTIMACIÓN DEL IMPACTO

El objetivo de esta actividad es determinar el alcance del daño producido sobre los activos de información en caso de llegarse a materializar una amenaza.

Para este caso se debe evaluar el grado de repercusión que pueda presentar cada activo, teniendo en cuenta las valoraciones vistas anteriormente como son: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad, haciendo uso de la siguiente tabla propuesta por Magerit.

Se debe tener en cuenta que los activos con calificación Media deberán ser reevaluados para mejorar, cambiar o adaptar nuevos controles, los de calificación Alta y muy alta deberán ser objeto atención Urgente.

Tabla 27. Valores de estimación de impacto

		DEGRADACION				
		1%	10%	50%	80%	100%
VALOR	MA	M	A	A	MA	MA
	A	B	M	M	A	A
	M	MB	B	B	M	M
	B	MB	MB	MB	B	B
	MB	MB	MB	MB	MB	MB

Fuente: Magerit V3, libro II, catálogo de elementos.

13.2.1 Impacto acumulado. Este es el impacto potencial al que está expuesto el sistema tomando como base los valores obtenidos de los activos y valoración de las amenazas, sin tener en cuenta las salvaguardas actuales. Estos se deben tener en cuenta con para una intervención inmediata por parte de la institución.

13.2.2 Impacto residual. Este resultado sale de combinar el valor de los activos, la valoración de las amenazas y la efectividad de los salvaguardas aplicadas; los activos con resultado muy bajo o bajo (o casillas en blanco), son riesgos con los que se puede convivir pero que se tuvieron en cuenta dentro de los controles, políticas de seguridad y recomendaciones.

Tabla 28. Valoración de impacto de los activos de la institución

ACTIVO	AMENAZA	IMPACTO CUMULADO					IMPACTO RESIDUAL				
		D	I	C	A	T	D	I	C	A	T
APLICACIONES INFORMATICAS	[E.1] Errores de los usuarios										
	[E.2] errores del administrador										
	[E.4] Errores de configuración										
	[E.14] Escapes de Información										
	[E.18] Destrucción de Información										
	[A.11] Acceso no Autorizado										
	[A.15] Modificación de la información										
SERVICIOS	[E.20] Vulnerabilidades de los programas										
	[A.5] Suplantación de la identidad del usuario										
	[A.8] Difusión de Software dañino										
	[A.24]Denegación de Servicios										

REDES DE COMUNICACIONES	[N.*] Desastres Naturales										
	[I.5]Avería de origen físico o lógico										
	[I.8]Fallo de Servicio de comunicaciones										
	[E.2] Errores del administrador										
	[A.4]Manipulación de Configuración.										
EQUIPAMIENTO INFORMATICO	[N.1] Fuego.										
	[I.2] Daños por Agua.										
	[I.5] Avería de origen físico o lógico										
	[E.23] Errores de mantenimiento/ actualización de equipos (hardware)										

Fuente: Autor

13.3 ESTIMACIÓN DEL RIESGO

Para este propósito, se hace uso de la siguiente escala cualitativa:

Tabla 29. Tabla valores de frecuencia para el riesgo

Valor			Criterio
100	Muy frecuente	MF	A diario
10	Frecuente	F	Mensualmente
1	Normal	FN	Una vez al año
1/10	Poco frecuente	PF	Cada varios años

Fuente: Magerit V3, Libro II.

Tabla 30. Criterios de valoración para estimación del riesgo

Riesgo		Frecuencia			
		PF	FN	F	MF
Impacto	MA	M	A	MA	MA
	A	B	A	MA	MA
	M	B	M	A	A
	B	MB	B	M	A
	MB	MB	MB	B	B

Fuente: Autor

En este punto, se tienen en cuenta los valores de la frecuencia de ocurrencia de cada amenaza frente a los activos e impacto acumulado porque necesitan atención inmediata.

Tabla 31. Lista de activos según el impacto, amenaza y riesgo

ACTIVO	AMENAZA	IMPACTO					F	RIESGO
		D	I	C	A	T		
APLICACIONES INFORMATICAS	[E.1] Errores de los usuarios						F	
	[E.2] errores del Administrador						FN	
	[E.4] Errores de configuración						FN	
	[E.14] Escapes de información						PF	
	[E.18] Destrucción de información						PF	
	[A.11] Acceso no autorizado						FN	
	[A.15] Modificación de la información						PF	
SERVICIOS	[E.20] Vulnerabilidades de los programas						PF	
	[A.5] Suplantación de la identidad del usuario						FN	
	[A.8]Difusión de Software Dañino						FN	

	[A.24]Denegación de Servicios						PF	
REDES DE COMUNICACIONES	[N.*] Desastres Naturales						PF	
	[I.5]Avería de origen físico o Lógico						FN	
	[I.8]Fallo de Servicio de comunicaciones						PF	
	[E.2] Errores del administrador						PF	
	[A.4]Manipulación de Configuración.						PF	
EQUIPAMIENTO INFORMATICO	[N.1] Fuego.						PF	
	[I.2] Daños por Agua.						PF	
	[I.5] Avería de origen físico o lógico						PF	
	[E.23] Errores de mantenimiento/ actualización de equipos						FN	

Fuente: Autor

13.4 INTERPRETACIÓN DE LOS RESULTADOS

Los controles son adaptados de acuerdo al resultado obtenido en las tablas de la actividad sobre estimación de riesgo, según las necesidades y características de cada activo.

Hardware:

- El mantenimiento preventivo y correctivo no se hace mediante programación adecuada, además el personal para tal fin no está bien definido y solo una persona lo hace teniendo a su cargo muchas otras funciones, situación que se hace más difícil para el cumplimiento normal.
- No hay criterios establecidos para los mantenimientos y actualizaciones, no se hace periódicamente ni existe un cronograma para hacerlo.
- No se tienen algunas restricciones como el uso y acceso de medios externos.
- No hay planes de contingencia ante averías o fallas temporales o definitivas en equipos imprescindibles dentro de la institución como servidores, por lo tanto se hace difícil una recuperación, cambio o renovación.
- No hay planes para dar de baja a equipos obsoletos.

Software:

- No todo el software es licenciado, solo aquel que es donado por alguna entidad gubernamental.
- No se tienen procedimientos definidos, ni registros de la aplicación de actualizaciones de software o parches de seguridad en los sistemas base críticos.

Redes:

- La red se encuentra segmentada física y lógicamente en la totalidad tanto en la sede central como en las otras dos sedes, esto permite administrar mejor los servicios a través del firewall y proxy.
- En la protección perimetral actualmente no hay un control de spam ni de antivirus generalizado para todos los equipos.
- Las dos sedes Garzón Moreno y Cristo Rey se comunican actualmente mediante radio a través de Nano Station M5 desde un punto central o minitore de la sede principal, el router y firewall actualmente instalado no soporta tráficos abundantes, lo que genera problemas en ocasiones cuando se accede a internet desde todos los puntos a la vez, se soluciona haciéndolo por horarios.
- No hay actualmente acceso a los servidores desde fuera de la red local o intranet, lo que permite minimizar los ataques externos, pero no se descartan los internos.

INSTALACIONES FÍSICAS:

- En la sede central el cableado y demás elementos físicos de las instalaciones tanto de datos como eléctricas cumplen los requerimientos mínimos de las normas actuales. En las otras dos sedes el cableado de red y eléctrico no está certificado por la norma a nivel de red de datos en ANSI/TIA 568A-B.
- No se cuentan con sistemas de protección y prevención de incendios, robo o acceso no autorizado para controlar el área física de los dispositivos e instalaciones, el sistema de aire acondicionado solo funciona en un sector.
- Los servidores no están localizados en un lugar adecuado para tal fin.

14. CONTROLES

14.1 ASPECTOS A CONTEMPLAR

Para especificar los controles según el PHVA en la Institución Educativa Luis Carlos Galán, se deben contemplar los aspectos que se mencionan a continuación:

Controles relacionados con terceros: Cuando exista la necesidad de otorgar acceso a terceras partes a la información de la Empresa, los Responsables de los Sistemas de Información, llevarán a cabo este proceso, debidamente autorizado por el propietario de la información, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- Los controles empleados por la tercera parte.
- La incidencia del acceso en la seguridad de la información en la Institución.
- Cumplimiento Institucional.

Acuerdos de control de accesos que contemplen:

- Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
- Proceso de autorización de accesos y privilegios de usuarios.
- Requerimiento para mantener actualizada una lista de personas autorizadas a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.
- Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.

- Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
- Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.
- Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
- Proceso claro y detallado de administración de cambios.
- Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.
- Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
- Controles que garanticen la protección contra software malicioso.
- Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.

14.2 MECANISMOS DE CONTROL DE ACTIVOS

14.2.1 Seguridad Física y Ambiental. Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información de los Sistemas de Información.

14.2.2 Controles de Acceso Físico. Los cuartos de comunicaciones y servidores se resguardarán mediante el empleo de controles de acceso físico, a fin de permitir el ingreso sólo al personal autorizado. Esta autorización es definida por el Comité de Seguridad Informática.

14.2.3 Protección de Oficinas, Recintos e Instalaciones. Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres

naturales o provocados por el hombre. Se tomará en cuenta las disposiciones y estándares en materia de sanidad y seguridad.

Se considerarán las amenazas de seguridad que representan los edificios y zonas aledañas.

14.2.4 Desarrollo de Tareas en Áreas Protegidas. Para incrementar la seguridad de las áreas protegidas, se establecerán controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí.

14.2.5 Seguridad del Cableado. El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará respalda a través de UPS y planta de energía con respaldo de un tiempo prudencial.

14.2.6 Mantenimiento de Equipos. La realización de tareas de mantenimiento preventivo al equipamiento, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Comité de Sistemas.

14.2.7 Controles Contra Software Malicioso. El Comité de Sistemas y de Seguridad Informática definirá controles de detección y prevención para la protección contra software malicioso y designará el personal encargado para dichos controles.

14.2.8 Controles de Redes. El Área de Sistemas definirá controles para garantizar la seguridad de la infraestructura de comunicaciones y los servicios conectados en las redes de la Institución, contra el acceso no autorizado.

Se podrán implementar controles para limitar la capacidad de conexión de los usuarios, de acuerdo a las políticas que se establecen a tal efecto. Dichos controles se podrán implementar en los firewalls

Se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos. Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino.

14.2.9 Administración de Medios Informáticos Removibles. Con el propósito de salvaguardar las copias de seguridad de los Sistemas de Información de la empresa, se dispone de un contrato con una empresa que custodia y salvaguarda la información que periódicamente es enviada según el procedimiento establecido para cada sistema.

14.2.10 Seguridad del Correo Electrónico. Las posibles vulnerabilidades a errores, por ejemplo, consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.

La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la terminal receptora o de la red a la que se encuentra conectada. Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.

El acceso de usuarios remotos a las cuentas de correo electrónico. El uso inadecuado por parte del personal.

14.2.11 Control de Acceso al Sistema Operativo. Identificación Automática de Terminales, El Área de TIC realizará una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso y uso del Sistema Operativo a través del Controlador de Dominio.

14.2.12 Procedimientos de Conexión de Terminales. El acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático será diseñado para minimizar la oportunidad de acceso no autorizado.

14.2.13 Identificación y Autenticación de los Usuarios. Todos los usuarios (incluido el personal de soporte técnico, los operarios, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo.

14.2.14 Sistema de Administración de Contraseñas. El sistema de administración de contraseñas debe:

- Sugerir el uso de contraseñas individuales para determinar responsabilidades.
- Permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
- Imponer una selección de contraseñas de calidad según lo señalado en el procedimiento establecido para el manejo y uso de contraseñas.
- Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto anterior.
- Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
- Mantener un registro de las últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.
- Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
- Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.
- Almacenar las contraseñas utilizando un algoritmo de cifrado.

- Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo claves de impresoras, hubs, routers, etc.).

- Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.

14.2.15 Control de Acceso a las Aplicaciones. Restricción del Acceso a la Información. Los usuarios de los sistemas de aplicación, incluyendo al personal de TIC, tendrán acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la Política de Control de Acceso definida, sobre la base de los requerimientos de cada aplicación, y conforme a los permisos otorgados de acuerdo al perfil solicitado por cada coordinador de área, Administradores o responsables de los Sistemas de Información.

- Validación de Datos de Entrada. Se validarán durante la etapa de diseño los controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando también datos permanentes y tablas de parámetros.

15. IDENTIFICACIÓN Y ANÁLISIS DE LOS REQUERIMIENTOS DE SEGURIDAD SEGÚN LA NORMA ISO27001:2013

Con el presente análisis se pretende conocer la distancia entre la situación actual y el SGSI proyectado.

15.1 ANÁLISIS DEL ANEXO A.

Controles de la norma ISO27001.

Tabla 32. Lista de controles

No	Título del Control	Descripción del control	Se cumple actualmente
A.5	POLITICA DE SEGURIDAD		Si/No/Parcialmente
A5.1	Políticas de seguridad de la información		
A.5.1.1	Documento de las políticas de seguridad de la información	Control La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.	NO
A.5.1.2	Revisión de las políticas de seguridad de la información	Control La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.	NO
A.6	OGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		

A.6.1	Organización interna		
A.6.1.1	Compromiso de la gerencia con la seguridad de la información	Control La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.	NO
A.6.1.2	Coordinación de la seguridad de información	Control Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.	NO
A.6.1.3	Asignación de responsabilidades de la seguridad de la información	Control Se deben definir claramente las responsabilidades de la seguridad de la información.	NO
A.6.1.4	Proceso de autorización para los servicios de procesamiento de información	Control Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información	Parcialmente
A.6.1.5	Acuerdos de confidencialidad	Control Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las	NO

		necesidades de la organización para la protección de la información.	
A.6.1.6	Contacto con autoridades	Control Se debe mantener los contactos apropiados con las autoridades relevantes.	Parcialmente
A.6.1.7	Contacto con grupos de interés especial	Control Se deben mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializada y asociaciones profesionales.	Parcialmente
A.6.1.8	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se debe revisar independientemente a intervalos planeados, o cuando ocurran cambios significativos para la implementación de la seguridad.	NO
A6.2	Entidades externas		
A.6.2.1	Identificación de riesgos relacionados con entidades externas	Control Se deben identificar los riesgos que corren la información y los medios de procesamiento de información de la organización y se deben implementar los controles apropiados antes de otorgar	NO

		acceso.	
A.6.2.2	Tratamiento de la seguridad cuando se trata con clientes	Control Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización.	NO
A.6.2.3	Tratamiento de la seguridad en contratos con terceras personas	Control Los acuerdos que involucran acceso, procesamiento, comunicación o manejo por parte de terceras personas a la información o los medios de procesamiento de información de la organización; agregar productos o servicios a los medios de procesamiento de la información deben abarcar los requerimientos de seguridad necesarios relevantes.	NO
A.7	Gestión de activos		
A.7.1	Responsabilidad por los activos		
A.7.1.1	Inventarios de activos	Control Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes	Parcialmente
A.7.1.2	Propiedad de los activos	Control	NO

		Toda la información y los activos asociados con los medios de procesamiento de la información deben ser 'propiedad' de una parte designada de organización.	
A.7.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.	NO
A.7.2	Clasificación de la información		
A.7.2.1	Lineamientos de clasificación	Control La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.	NO
A.7.2.2	Etiquetado y manejo de la información	Control Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.	NO
A.8	Durante el empleo		
A.8.1	Antes del empleo		
A.8.1.1	Roles y responsabilidades	Control Se deben definir y documentar los roles y responsabilidades de seguridad de los	NO

		empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.	
A.8.1.2	Selección	Control Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y	NO
A.8.1.3	Términos y condiciones de empleo	Control Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información.	SI
A.8.2	Durante el empleo		
A.8.2.1	Gestión de responsabilidades	Control La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.	SI

A.8.2.2	Capacitación y educación en seguridad de la información	Control Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.	NO
A.8.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.	Parcialmente
A.8.3	Terminación o cambio del empleo		
A.8.3.1	Responsabilidades de terminación	Control Se deben definir y asignar claramente las responsabilidades para realizar la terminación o cambio del empleo.	SI
A.8.3.2	Devolución de activos	Control Todos los empleados, contratistas y terceros deben devolver todos los activos de la organización que estén en su posesión a la terminación de su empleo, contrato o acuerdo.	Parcialmente
A.8.3.3	Eliminación de derechos de acceso	Control Los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de	Parcialmente

		la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.	
A.9	Seguridad física y ambiental		
A9.1	Áreas seguras		
A9.1.1	Perímetro de seguridad física	Control Se deben utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.	NO
A9.1.2	Controles de entrada físicos	Control Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.	NO
A9.1.3	Seguridad de oficinas, habitaciones y medios	Control Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.	Parcialmente
A9.1.4	Protección contra amenazas externas y ambientales	Control Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.	Parcialmente
A9.1.5	Trabajo en áreas seguras	Control Se debe diseñar y aplicar protección física y	NO

		lineamientos para trabajar en áreas seguras.	
A9.1.6	Áreas de acceso público, entrega y carga	Control Se deben controlar los puntos de acceso como las áreas de entrega y descarga y otros puntos donde personas no-autorizadas pueden ingresar a los locales, y cuando fuese posible, se deben aislar de los medios de procesamiento de la información para evitar un acceso no autorizado.	NO
A9.2			
A9.2.1	Ubicación y protección de equipos	Control los equipo de deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno y las oportunidades de acceso no autorizado.	NO
A9.2.2	Servicio de suministros	Control los equipos de deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas en los servicios de suministro	Parcialmente
A9.2.3	Seguridad del cableado	Control el cableado de energía eléctrica y telecomunicaciones que trasporta datos o presta soporte a los servicios de información deben estar protegidos contra interrupciones o daños	Parcialmente

A9.2.4	Mantenimiento de los equipos	Control El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad	Parcialmente
A9.2.5	Seguridad de los equipos fuera de las instalaciones	Control Se debe aplicar seguridad al equipo fuera-del local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.	NO
A9.2.6	Seguridad de la reutilización o eliminación de los equipos	Control Todos los ítems de equipo que contengan medios de almacenaje deben ser chequeados para asegurar que se haya removido o sobre-escrito de manera segura cualquier data confidencial y software con licencia antes de su eliminación.	NO
A9.2.7	Retiro de activos	Control Equipos, información o software no deben ser sacados fuera de la propiedad sin previa autorización.	NO
A10	GESTIÓN DE COMUNICACIONES Y OPERACIONES		
A10.1	Procedimientos operacionales y responsabilidades.		
A10.1.1	Documentación de los procedimientos de operación.	Los procedimientos de operación se deben documentar, mantener y estar disponibles	NO

		para todos los usuarios que los necesiten.	
A10.1.2	Gestión del cambio.	Se debe controlar los cambios en los servicios y los sistemas de procesamiento de información.	NO
A10.1.3	Distribución de funciones.	Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización.	NO
A10.1.4	Separación de las instalaciones de desarrollo, ensayo y operación.	Las instalaciones de desarrollo, ensayo y operación deben estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.	NO
A10.2	Gestión de la prestación de los servicios por terceras partes.		
A10.2.1	Prestación del servicio.	Se debe garantizar que los controles de seguridad, las definiciones del servicio y los niveles de prestación del servicio incluidos en el acuerdo, sean implementados, mantenidos y operados por las terceras partes.	NO
A10.2.2	Monitoreo y revisión de los servicios por terceras partes.	Los servicios, reportes y registros suministrados por terceras partes se deben controlar y revisar con regularidad y las auditorias se deben llevar a cabo a intervalos regulares.	NO

A10.2.3	Gestión de los cambios en los servicios por terceras partes.	Los cambios de la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas existentes de seguridad de la información, en los procedimientos y controles se deben gestionar teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la revaluación de los riesgos.	NO
A10.3	Protección contra códigos maliciosos y móviles.		
A10.3.1	Gestión de la capacidad.	Se debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.	NO
A10.3.2	Aceptación del sistema.	Se deben establecer criterios de aceptación para Sistemas de Información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.	Parcialmente
A10.4	Protección contra códigos maliciosos y móviles.		
A10.4.1	Controles contra códigos maliciosos.	Se debe implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así	Parcialmente

		como procedimientos adecuados de concientización de los usuarios.	
A10.4.2	Controles contra códigos móviles.	Cuando se autoriza la utilización de códigos móviles, la configuración debe asegurar que dichos códigos operan de acuerdo con la política de seguridad claramente definida, y se debe evitar la ejecución de los códigos móviles no autorizados.	NO
A10.5	Respaldo		
A10.5.1	Respaldo de la información.	Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.	Parcialmente
A10.6	Gestión de la seguridad de las redes		
A10.6.1	Controles de la redes.	Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.	Parcialmente
A10.6.2	Seguridad de los servicios de la red.	En cualquier acuerdo sobre los servicios de la red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la organización o se contratan externamente.	Parcialmente

A10.7	Manejo de los Medios.		
A10.7.1	Gestión de los medios removibles.	Se deben establecer procedimientos para la gestión de medios removibles.	
A10.7.2	Eliminación de los medios.	Cuando ya no se requieran estos medios, su eliminación se debe hacer en forma segura y sin riesgo, utilizando los procedimientos formales.	NO
A10.7.3	Procedimientos para el manejo de la información.	Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.	NO
A10.7.4	Seguridad de la documentación del sistema.	La documentación del sistema debe estar protegida contra acceso no autorizado.	Parcialmente
A10.8	Intercambio de la información.		
A10.8.1	Políticas y procedimientos para el intercambio de información.	Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación.	NO
A10.8.2	Acuerdos para el intercambio.	Se deben establecer acuerdos para el intercambio de la información y el software entre la organización y partes externas.	NO
A10.8.3	Medios físicos en tránsito.	Los medios que contienen información se deben proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de	NO

		los límites físicos de la organización.	
A10.8.4	Mensajería electrónica.	La información contenida en la mensajería electrónica debe tener la protección adecuada.	NO
A10.8.5	Sistemas de Información del negocio.	Se deben establecer, desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los Sistemas de Información del negocio.	NO
A10.9	Servicios de comercio electrónico.		
A10.9.1	Comercio electrónico.	La información involucrada en el comercio electrónico que se transmite por las redes públicas debe estar protegida contra actividades fraudulentas, disputas de contratos y divulgación o modificación no autorizada.	NO
A10.9.2	Transacciones en línea.	La información involucrada en las transacciones en línea debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración, divulgación, duplicación o repetición no autorizada del mensaje.	NO
A10.9.3	Información disponible al público.	La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no autorizada.	Parcialmente

A10.10	Monitoreo		
A10.10.1	Registro de auditorías.	Se debe elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoria de las actividades de los usuarios, la excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.	NO
A10.10.2	Monitoreo del uso del sistema.	Se deben establecer procedimientos para el monitoreo de uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deben revisar con regularidad.	NO
A10.10.3	Protección de la información del registro.	Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados.	NO
A10.10.4	Registros del administrador y del operador.	Se deben registrar las actividades tanto del operador como del administrador del sistema.	NO
A10.10.5	Registros de falla.	Las fallas se deben registrar y analizar, y se deben tomar las acciones adecuadas.	NO
A10.10.6	Sincronización de relojes.	Los relojes de todos los sistemas de procesamiento de información pertinente dentro de la organización o del dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta y acordada.	NO
A11			

A11.1	Requisitos del negocio para el control de acceso.		
A11.1.1	Política de control de acceso.	Se debe establecer, documentar y revisar la política de control de acceso con base a los requisitos del negocio y de la seguridad para el acceso.	Parcialmente
A11.2	Gestión del acceso de usuarios.		
A11.2.1	Registro de usuarios.	Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.	NO
A11.2.2	Gestión de privilegios.	Se debe restringir y controlar la asignación y uso de privilegios.	Parcialmente
A11.2.3	Gestión de contraseñas para usuarios.	La asignación de contraseñas se debe controlar a través de un proceso formal de gestión.	Parcialmente
A11.2.4	Revisión de los derechos de acceso de los usuarios.	La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.	NO
A11.3	Responsabilidades de los usuarios		
A11.3.1	Uso de contraseñas.	Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas.	NO

A11.3.2	Equipo de usuario desatendido.	Los usuarios deben asegurarse de que los equipos desatendidos se las da la protección adecuada.	NO
A11.3.3	Política de escritorio despeja y pantalla despejada.	Se debe adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.	NO
A11.4	Control de acceso a las redes		
A11.4.1	Política de uso de servicios de red.	Los usuarios solo deben tener acceso a los servicios para cuyo uso están específicamente autorizados.	Parcialmente
A11.4.2	Autenticación de usuarios para conexiones externas.	Se deben emplear métodos adecuados de autenticación para controlar el acceso de usuarios remotos.	Parcialmente
A11.4.3	Identificación de los equipos en las redes.	La identificación automática de los equipos se debe considerar un medio para autenticar conexiones de equipos y ubicaciones específicas.	SI
A11.4.4	Protección de los puestos de configuración y diagnostico remoto.	El acceso lógico y físico a los puertos de configuración y de diagnóstico debe estar controlado.	NO
A11.4.5	Separación de las redes.	En las redes se deben separar los grupos de servicios de información, usuarios y Sistemas de Información.	Parcialmente
A11.4.6	Control de conexión a las redes.	Para redes compartidas, especialmente para aquellas que se extienden más allá de	Parcialmente

		las fronteras de la organización, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control de acceso y los requisitos de aplicación del negocio (véase el numeral 11.1)	
A11.4.7	Control de enrutamiento en la red.	Se deben implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control del acceso a de las aplicaciones.	Parcialmente
A11.5	Control de acceso al sistema operativo.		
A11.5.1	Procedimientos de ingreso seguro.	El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de inicio seguro.	NO
A11.5.2	Identificación y autenticación de usuarios.	Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.	NO
A11.5.3	Sistema de gestión de contraseñas.	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	NO
A11.5.4	Uso de las utilidades del sistema.	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden	NO

		anular los controles del sistema y de la aplicación.	
A11.5.5	Tiempo de inactividad de la sesión.	Las sesiones inactivas se deben suspender después de un periodo de inactividad.	Parcialmente
A11.5.6	Limitación del tiempo de conexión.	Se deben utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo.	NO
A11.6	Control de acceso a las aplicaciones y a la información.		
A11.6.1	Restricciones de acceso a la información.	Se debe restringir el acceso a la información y las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida en el control de acceso.	Parcialmente
A11.6.2	Aislamiento de sistemas sensibles.	Los sistemas sensibles deben tener un entorno informático dedicado (aislados).	NO
A11.7	Computación móvil y trabajo remoto.		
A11.7.1	Computación y comunicaciones móviles.	Se debe establecer una política formal y se deben adoptar las medidas de seguridad apropiadas para la protección contra riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.	NO
A11.7.2	Trabajo remoto.	Se deben desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de	NO

		trabajo remoto.	
A12			
A12.1	Requisitos de seguridad de los Sistemas de Información.		
A12.1.1	Análisis y especificación de los requisitos de seguridad.	Las declaraciones sobre los requisitos del negocio para nuevos Sistemas de Información o mejoras de los sistemas existentes deben especificar los requisitos para los controles de seguridad.	NO
A12.2	Procesamiento correcto de las aplicaciones.		
12.2.1	Validación de los datos de entrada.	Se deben validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados.	NO
12.2.2	Control de procesamiento interno.	Se deben incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados.	NO
12.2.3	Integridad del mensaje.	Se deben identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.	NO
12.2.4	Validación de los datos de salida.	Se deben validar los datos de salida de una aplicación para asegurar que el procesamiento de la información	NO

		almacenada es correcto y adecuado a las circunstancias.	
A12.3	Controles Criptográficos.		
12.3.1	Política sobre el uso de controles criptográficos.	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	NO
12.3.2	Gestión de llaves.	Se debe implementar un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas por parte de la organización.	NO
A12.4	Seguridad de los archivos del sistema.		
12.4.1	Control del software operativo.	Se deben implementar procedimientos para controlar la instalación de software en los sistemas operativos.	NO
12.4.2	Protección de los datos de prueba del sistema.	Los datos de prueba deben seleccionarse cuidadosamente, así como protegerse y controlarse.	NO
12.4.3	Control de acceso al código fuente de los programas.	Se debe restringir el acceso al código fuente de los programas.	NO
A12.5	Seguridad en los procesos de desarrollo y soporte		
12.5.1	Procedimientos de control de cambios.	Se debe controlar la implementación de cambios utilizando procedimientos formales de control de cambios.	Parcialmente
12.5.2	Revisión técnica de las	Cuando se cambias los sistemas operativos,	Parcialmente

	aplicaciones después de los cambios en el sistema operativo.	las aplicaciones críticas para el negocio se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.	
12.5.3	Restricciones en los cambios a los paquetes del software.	Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	NO
12.5.4	Fuga de información.	Se debe evitar las oportunidades para que se produzca fuga de información.	NO
12.5.5	Desarrollo de software contratado externamente.	La organización debe supervisar y monitorear el desarrollo de software contratado externamente.	NO
A12.6	Gestión de la vulnerabilidad técnica.		
12.6.1	Control de vulnerabilidades técnicas.	Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los Sistemas de Información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.	Parcialmente
A13			
A13.1	Reporte sobre los eventos y las debilidades de la seguridad de		

	la información.		
13.1.1	Reporte sobre los eventos de seguridad de la información.	Los eventos de seguridad de la información se deben informar atreves de los canales de gestión apropiados tan pronto como sea posible.	NO
13.1.2	Reporte sobre las debilidades de la seguridad.	Se debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.	NO
13.2	Gestión de los incidentes y las mejoras en la seguridad de la información.		
13.2.1	Responsabilidades y procedimientos.	Se deben establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	NO
13.2.2	Aprendizaje debido a los incidentes de seguridad de la información.	Deben existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.	NO
13.2.3	Recolección de evidencia.	Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y	NO

		presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.	
A14			
A14.1	Aspectos de seguridad de la información, de la gestión de la continuidad del negocio.		
14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	Se debe desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.	NO
14.1.2	Continuidad del negocio y evaluación de riesgos.	Se debe identificar los eventos que puedan ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.	NO
14.1.3	Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información.	Se deben desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos críticos para el negocio.	NO
14.1.4	Estructura para la planificación de la continuidad del negocio.	Se debe mantener una sola estructura de los planes de continuidad del negocio, para	NO

		asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento.	
14.1.5	Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio.	Los planes de continuidad del negocio se deben someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.	NO
A15			
A15.1	Cumplimiento de los requisitos legales.		
15.1.1	Identificación de la legislación aplicable.	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada Sistema de Información y para la organización.	Parcialmente
15.1.2	Derechos de la propiedad intelectual (DPI).	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.	Parcialmente
15.1.3	Protección de los registros de la organización.	Los registros importantes se deben proteger contra perdida, destrucción y falsificación,	NO

		de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio.	
15.1.4	Protección de los datos y privacidad de la información personal.	Se debe garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes, si se aplica, con las clausulas del contrato.	NO
15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información.	Se debe disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.	NO
15.1.6	Reglamentación de los controles criptográficos.	Se deben utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.	NO
A15.2	Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico.		
15.2.1	Cumplimiento con las políticas y normas de seguridad.	Los directores deben garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr los cumplimientos con las políticas y las normas de seguridad.	NO
15.2.2	Verificación del cumplimiento técnico.	Los Sistemas de Información se deben verificar periódicamente para verificar el cumplimiento con las normas de implementación de la seguridad.	NO
A15.3	Consideraciones de la auditoria de los Sistemas de Información.		

15.3.1	Controles de auditoria de Los Sistemas de Información.	Los requisitos y las actividades de auditoria que implican verificaciones de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.	NO
15.3.2	Protección de las herramientas de auditoria de los Sistemas de Información.	Se debe proteger el acceso a las herramientas de auditoria de los Sistemas de Información para evitar su uso inadecuado o ponerlas en peligro	NO

Fuente: ISO/MEC/IEC 27001, Anexo A y complementado.

16. POLITICAS DE SEGURIDAD INFORMÁTICA

Las políticas establecidas en el presente documento constituyen un referente importante para la conservación de los activos informáticos de la institución Educativa Luis Carlos Galán, junto con documentos, archivos y demás componentes que hacen parte de la información crucial para continuar el objetivo del negocio.

Finalidad de la política

Al establecer las políticas de seguridad informática se da paso a la búsqueda de la integridad, confiabilidad y autenticidad de la información como puntos de partida para el buen funcionamiento de la institución pública, además de evitar problemas a mediano y largo plazo, dándole mayor confiabilidad a todos los procesos internos.

16.1 SEGURIDAD RELACIONADA AL PERSONAL

16.1.1 Políticas para Funcionarios. Los usuarios y servidores de la Institución Educativa Luis Carlos Galán, deben preservar y proteger los registros y la información utilizada en la infraestructura tecnológica, de igual forma protegerán la información almacenada o transmitida ya sea dentro de la red interna institucional, a otras dependencias, a sedes alternas o redes externas.

- Toda información producida y/o manipulada por los funcionarios se considera propiedad la Institución Educativa Luis Carlos Galán.
- Todos los archivos de computadores que sean proporcionados por personal externo o interno (programas, software, bases de datos, documentos y hojas de cálculo) que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus, utilizando el software antivirus autorizado en la institución antes de ejecutarse.

- La información manipulada por el funcionario de la Institución no debe ser divulgada a terceros, salvo autorización o solicitud expresa.
- Cada usuario es responsable de las acciones realizadas en la red institucional.
- Los archivos e información que cada docente ingrese a los sistemas de plataforma virtual, pasan a ser propiedad de la institución solo fines educativos y no lucrativos.
- Los usuarios con cuenta de administrador que tienen acceso a información crucial de bases de datos y demás sistemas, no pueden extraer dicha información sin autorización.

16.1.2 Políticas de Capacitación. Todo el personal de la institución debe ser capacitado en el uso correcto de las redes de datos y Sistemas de Información, teniendo en cuenta la seguridad de los mismos.

- Tomar medidas para capacitar a todo el personal en el sentido de no comprometer la seguridad y a la vez los activos de la institución.
- Establecer obligatoriedad en la asistencia a las capacitaciones por parte del Rector de la institución.

16.1.3 Políticas de control de Incidentes. Se efectuarán copias de seguridad o back-ups diariamente en servidores y algunos computadores de oficina, las copias se guardarán directamente en el NAS rotuladas con fecha y hora.

- Todo incidente u ocurrencia de accidente de seguridad informática debe ser reportado oficialmente al jefe de sistemas de la institución.
- Las solicitudes de atención a usuarios de los Sistemas de Información se hacen vía correo electrónico al administrador para ser atendidas en el menor tiempo posible.
- El administrador de sistemas dará el soporte necesario y recurrirá a terceros

cuando sea necesario, dejando registrado el incidente.

16.2 SEGURIDAD LÓGICA

16.2.1 Políticas de Control de Acceso. Todo funcionario nuevo debe ser reportado con la debida autorización al jefe de sistemas para la respectiva creación de autenticación en los sistemas.

- Cada funcionario debe utilizar su propio rol y autenticación asignado, no se autoriza el intercambio de claves y usuarios entre ellos.
- Cada uno se hace responsable de los datos de ingreso a cada Sistema de Información e infraestructura de red.
- En el caso de retiro de un docente o funcionario, el rector, coordinador o secretaria debe informar de inmediato al jefe de sistemas para retirarlo o desactivarlo.

16.2.2 Políticas de Administración de acceso a usuarios. Son usuarios de la red de la institución los alumnos, docentes, contratistas, administrativos y en general cualquier persona que haga uso de los servicios de la red.

- El jefe de sistemas es la persona encargada de generar y administrar las cuentas de usuario para el logueo de los mismos en todos los sistemas de la institución.
- Los estudiantes no tienen autorización para todos los sistemas ni con roles completos, solo tiene autorización para algunas consultas y a la red por horarios.
- Todos los sistemas de autenticación deberán tener un sistema de asignación de contraseñas fuertes según los requerimientos mínimos.
- Evitar la reutilización de las contraseñas, para ello contar en el sistema con un historial interno de las mismas y evitar volver a usarlas.

- Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
- Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo claves de
- impresoras, hubs, routers, etc.).

16.2.3 Políticas Creación de contraseñas fuertes. Para todas las contraseñas creadas, deberán hacerse teniendo en cuenta los siguientes requisitos mínimos:

- Usar una combinación alfanumérica
- Mínimo una mayúscula, una minúscula, un carácter especial y un número
- La contraseña debe tener una longitud mínima de 8 caracteres.
- La contraseña debe tener un periodo de vigencia, luego deberá ser cambiada por una nueva y diferente a la anterior.
- No usar datos personales, números de identificación, fechas de nacimiento ni nombres normales o del común para crear las contraseñas, éstas no deben tener ningún significado en común.

16.2.4 Políticas Responsabilidades de los usuarios. El uso y responsabilidad de la cuenta de usuario asignada por el jefe de sistemas, es de cada uno de forma individual.

- Cada usuario debe evitar guardar en algún medio físico o magnético la contraseña asignada para evitar suplantación.
- La institución educativa no se hace responsable de la información personal, cada usuario es responsable de ello.
- Los usuarios deben reportar al jefe de sistemas si conocen cualquier anomalía, falla o ataque que vulnere o ponga en riesgo la seguridad informática de la institución para que se tomen medidas.

- Todos los usuarios de la institución deben colaborar con la seguridad de la información, cumpliendo las políticas creadas para tal fin.

16.2.5 Políticas de Acceso a terceros. Todo el personal que tenga alguna relación con la institución como contratistas, personal temporal, empleados de Secretaría de Educación y Ministerio de Educación enviados para cumplir funciones esporádicas o de auditoría, son considerados como terceros.

- El acceso para el personal de terceros será restringido y temporal, después de cumplir con los permisos correspondientes ante la oficina de rectoría y pasar por el jefe de sistemas.
- Los usuarios terceros deben acatar todas las disposiciones y normas internas de la institución educativa Luis Carlos Galán.

16.2.6 Políticas de Acceso a la red. Se prohíbe y es considerada una falta grave dentro de la institución educativa la exploración por software de ataque o por medios físicos a la infraestructura de la red interna.

- Todo usuario para ingresar a la red interna, debe solicitar autorización con su hardware al jefe de sistemas.
- La oficina de sistemas de la institución, debe establecer filtros para controlar el acceso tanto a la red interna como externa y viceversa, con el propósito de tratar de proteger la infraestructura de ataques.
- Se deberán guardar periódicamente registros o logs de acceso a los sistemas.

16.2.7 Políticas para Backups. Establecer controles de verificación de backups de todos los sistemas existentes en la institución, así mismo de los servicios en la nube a través de Hosting privado, con el propósito de comprobar que las copias se estén efectuando de acuerdo a su programación.

- Establecer un medio de almacenamiento externo y seguro para los backups,

para propiciar una correcta recuperación en caso necesario.

- El área de sistemas será la responsable de mantener los medios de almacenamiento de forma segura.
- Documentar cualquier proceso de recuperación si lo hubiere.

16.2.8 Políticas para Servidores. La instalación, configuración, reinstalación y recuperación de sistemas operativos de servidores es labor exclusiva del área de sistemas y de su administrador.

- Se darán permisos de acuerdo al perfil de cada usuario para acceso a los servidores.
- El jefe de sistemas deberá establecer y activar mecanismos de seguridad en cada servidor para ayudar a protegerlo como firewall y reglas internas.

16.2.9 Políticas para equipos de cómputo o terminales. Ningún usuario está autorizado para remover sellos de garantía ni cables de los equipos tanto de salas de cómputo como de uso individual en oficinas, esa es responsabilidad del área de sistemas.

- Es responsabilidad de cada usuario almacenar solo información de índole laboral relacionada con la institución educativa.
- Se prohíbe destapar o manipular internamente cualquier dispositivo, computador o periférico de la institución, esta labor solo es autorizada por la oficina de sistemas.
- El préstamo y asignación de tablets o portátiles para llevarlos fuera de la institución solo se hace con autorización de las directivas de la institución de forma escrita hacia la oficina de sistemas, se hace la entrega a través del acta respectiva.
- Cualquier daño o situación anormal de un equipo de cómputo debe reportarse al área de sistemas de forma inmediata, para tomar medidas al respecto.

16.3 RESPONSABILIDADES Y PROCEDIMIENTOS

- La oficina de sistemas es la encargada de planear los mantenimientos correctivos y preventivos, bien sea ejecutados por la misma oficina o contratados con terceros, sin perjudicar el horario normal de trabajo o jornada escolar.
- Todos los equipos de las salas de cómputo y oficinas al culminar la jornada laboral, deben quedar completamente apagados y aislados de la corriente para evitar daños por rayos y caídas de energía, situación que es frecuenta en esta zona.

16.3.1 Políticas de protección contra software malicioso. No se debe usar software que no esté autorizado o licenciado dentro de la institución educativa.

- Dejar de usar cualquier computador o memoria externa que se encuentre contagiada de virus o software malicioso, reportarse a la oficina de sistemas para realizar el correspondiente proceso de limpieza.
- Las directivas deben aprobar anualmente la adquisición de software antivirus licenciado para cada uno de los equipos de cómputo, principalmente en las oficinas, así mismo instalar software antimalware de licencia libre para ayudar a mantener limpios de programas maliciosos.
- Mantener actualizado el software antivirus y antimalware.

16.3.2 Políticas de mantenimiento. Solo el personal autorizado por la oficina de sistemas se hará cargo del mantenimiento.

- Se debe llevar una hoja de vida de cada equipo de cómputo para llevar control de los cambios realizados y los mantenimientos ejecutados.
- Dar aviso con anterioridad al encargado de la oficina respectiva donde se vaya a realizar el mantenimiento.

16.4 SEGURIDAD FÍSICA

16.4.1 Políticas de seguridad física en los equipos. Todos los servidores deben reubicarse en un mismo sitio debidamente protegidos del acceso directo y físico.

- Para ingresar al área donde se encuentran los controles y servidores, se deberá solicitar autorización al jefe de sistemas.
- Los equipos de cómputo, cables, UPS, subestación eléctrica, aires acondicionados, dispositivos de almacenamiento y de comunicación móvil o inalámbrica, deben estar amparados en pólizas contra robo, pérdida, daño o acceso no autorizado. Además, no será permitido el consumo de líquidos, alimentos, ni humo dentro de los centros de cómputo o salas donde reposen los equipos. [ISO/IEC 27001:2005 A.9.2]

16.5 SEGURIDAD LEGAL

16.5.1 Políticas de licenciamiento de software. Todo el software instalado y de uso dentro de la institución debe estar licenciado, a excepción de software libre utilizado con fines educativos.

- Todos los programas o software son instalados por la oficina de sistemas.
- Se debe mantener en la oficina de sistemas un inventario actualizado de software y hardware instalado.

17. DECLARACIÓN DE APLICABILIDAD

Teniendo en cuenta los controles de la ISO 27001 Anexo A, se analizan y establecen aquellos que son aplicables al proyecto SGSI de la institución educativa Luis Carlos Galán de Villagarzón Putumayo.

Tabla 33. Lista de controles aplicables

ISO 27001 SOA				
No	**Título del Control**	**Descripción del control**	**Implementación SI/NO**	**Justificación u observaciones**
A.5	POLITICA DE SEGURIDAD			
A5.1	Políticas de seguridad de la información			
A.5.1.1	Documento de las políticas de seguridad de la información	Control La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.	SI	La gerencia debe liderar el proceso.
A.5.1.2	Revisión de las políticas de seguridad de la información	Control La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios	SI	Se debe mejorar continuamente el SGSI.

		significativos para asegurar la continua idoneidad, eficiencia y efectividad.		
A.6	OGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
A.6.1	Organización interna			
A.6.1.1	Compromiso de la gerencia con la seguridad de la información	Control La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.	SI	El compromiso de la gerencia en el proceso debe ser decidido.
A.6.1.2	Coordinación de la seguridad de información	Control Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.	SI	Los funcionarios forman parte activa del proceso.
A.6.1.3	Asignación de responsabilidades de la seguridad de la información	Control Se deben definir claramente las responsabilidades de la seguridad de la información.	SI	
A.6.1.4	Proceso de autorización para	Control Se debe definir e implementar un	SI	

	los servicios de procesamiento de información	proceso de autorización gerencial para los nuevos medios de procesamiento de información		
A.6.1.5	Acuerdos de confidencialidad	Control Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.	NO	Deben existir acuerdos de confidencialidad para proteger la información.
A.6.1.6	Contacto con autoridades	Control Se deben mantener los contactos apropiados con las autoridades relevantes.	SI	Mantener contacto a nivel de jerarquía.
A.6.1.7	Contacto con grupos de interés especial	Control Se deben mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializada y asociaciones profesionales.	SI	Mantenerse informados sobre los últimos acontecimientos de seguridad.
A.6.1.8	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y	SI	Cumplir con las políticas de auditoría interna.

		procedimientos para la seguridad de la información) se debe revisar independientemente a intervalos planeados, o cuando ocurran cambios significativos para la implementación de la seguridad.		
A6.2	Entidades externas			
A.6.2.1	Identificación de riesgos relacionados con entidades externas	Control Se deben identificar los riesgos que corren la información y los medios de procesamiento de información de la organización y se deben implementar los controles apropiados antes de otorgar acceso.	SI	Controlar el acceso externo cuando sea autorizado.
A.6.2.2	Tratamiento de la seguridad cuando se trata con clientes	Control Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización.	SI	Controlar el acceso.
A.6.2.3	Tratamiento de la seguridad en contratos con terceras personas	Control Los acuerdos que involucran acceso, procesamiento, comunicación o manejo por parte de terceras	SI	Control a terceros.

		personas a la información o los medios de procesamiento de información de la organización; agregar productos o servicios a los medios de procesamiento de la información deben abarcar los requerimientos de seguridad necesarios relevantes		
A.7	GESTIÓN DE ACTIVOS			
A.7.1	Responsabilidad por los activos			
A.7.1.1	Inventarios de activos	Control Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes	SI	Se deben identificar los activos.
A.7.1.2	Propiedad de los activos	Control Toda la información y los activos asociados con los medios de procesamiento de la información deben ser 'propiedad' de una parte designada de a organización.	SI	Valorar los activos.
A.7.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información	SI	Crear e implementar controles asociados.

		y los activos asociados con los medios de procesamiento de la información.		
A.7.2	Clasificación de la información			
A.7.2.1	Lineamientos de clasificación	Control La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.	NO	N/A
A.7.2.2	Etiquetado y manejo de la información	Control Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.	NO	N/A
A.8	DURANTE EL EMPLEO			
A.8.1	Antes del empleo			
A.8.1.1	Roles y responsabilidades	Control Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de	SI	Establecer políticas según los roles.

		la seguridad de información de la organización.		
A.8.1.2	Selección	Control Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y	NO	La contratación de personal no la hace directamente la institución, sino la entidad certificada para tal fin.
A.8.1.3	Términos y condiciones de empleo	Control Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información.	NO	N/A
A.8.2	Durante el empleo			

A.8.2.1	Gestión de responsabilidades	Control La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.	SI	Cumplir con las políticas para cada empleado o tercero.
A.8.2.2	Capacitación y educación en seguridad de la información	Control Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.	SI	Es necesario que todos conozcan el plan propuesto y las políticas definidas en seguridad.
A.8.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.	SI	El rector debe hacer cumplir las reglas y políticas.
A.8.3	Terminación o cambio del empleo			
A.8.3.1	Responsabilidades de terminación	Control Se deben definir y asignar	NO	N/A

		claramente las responsabilidades para realizar la terminación o cambio del empleo.		
A.8.3.2	Devolución de activos	Control Todos los empleados, contratistas y terceros deben devolver todos los activos de la organización que estén en su posesión a la terminación de su empleo, contrato o acuerdo.	SI	Los activos devolutivos deben permanecer o volver a la institución.
A.8.3.3	Eliminación de derechos de acceso	Control Los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.	SI	Se deben cambiar o controlar las cuentas de acceso de las personas que salen o dejan de laborar en lla institución.
A.9	SEGURIDAD FÍSICA Y AMBIENTAL			
A9.1	Áreas seguras			
A9.1.1	Perímetro de seguridad física	Control Se debe utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas)	SI	Actualmente los equipos de cómputo o dispositivos especiales no tienen acceso restringido.

		para proteger áreas que contienen información y medios de procesamiento de información.		
A9.1.2	Controles de entrada físicos	Control Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.	SI	Establecer y crear políticas de control a las áreas físicas.
A9.1.3	Seguridad de oficinas, habitaciones y medios	Control Se debe diseñar y aplicar seguridad física en las oficinas.	SI	Establecer controles de seguridad en estas áreas.
A9.1.4	Protección contra amenazas externas y ambientales	Control Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.	SI	Adquirir e instalar mecanismos de protección.
A9.1.5	Trabajo en áreas seguras	Control Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras.	NO	No hay diferenciación de estas áreas.
A9.1.6	Áreas de acceso público, entrega y carga	Control Se deben controlar los puntos de acceso como las áreas de	NO	No se maneja carga.

		entrega y descarga y otros puntos donde personas no-autorizadas pueden ingresar a los locales, y cuando fuese posible, se deben aislar de los medios de procesamiento de la información para evitar un acceso no autorizado.		
A9.2				
A9.2.1	Ubicación y protección de equipos	Control Los equipos de deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno y las oportunidades de acceso no autorizado.	SI	No hay una ubicación de equipos de forma segura.
A9.2.2	Servicio de suministros	Control Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas en los servicios de suministro	SI	No existen suficientes UPS.
A9.2.3	Seguridad del cableado	Control El cableado de energía eléctrica y telecomunicaciones que trasporta datos o presta soporte a los servicios de información deben estar protegidos contra	SI	No hay protección física en todas las conexiones.

		interrupciones o daños		
A9.2.4	Mantenimiento de los equipos	Control El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad	SI	No hay planificación de mantenimientos.
A9.2.5	Seguridad de los equipos fuera de las instalaciones	Control Se debe aplicar seguridad al equipo fuera-del- local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.	SI	
A9.2.6	Seguridad de la reutilización o eliminación de los equipos	Control Todos los ítems de equipo que contengan medios de almacenaje deben ser chequeados para asegurar que se haya removido o sobre-escrito de manera segura cualquier data confidencial y software con licencia antes de su eliminación.	SI	No hay control de la baja de equipos y software.
A9.2.7	Retiro de activos	Control Equipos, información o software no deben ser sacados fuera de la propiedad sin previa	SI	No hay control de la baja de activos.

		autorización.		
A10	GESTIÓN DE COMUNICACIONES Y OPERACIONES			
A10.1	Procedimientos operacionales y responsabilidades.			
A10.1.1	Documentación de los procedimientos de operación.	Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.	SI	No existe documentación de procedimientos.
A10.1.2	Gestión del cambio.	Se debe controlar los cambios en los servicios y los sistemas de procesamiento de información.	SI	No hay control de las modificaciones del software.
A10.1.3	Distribución de funciones.	Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización.	NO	El bajo número de personal en sistemas no lo permite.
A10.1.4	Separación de las instalaciones de desarrollo, ensayo y operación.	Las instalaciones de desarrollo, ensayo y operación deben estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.	NO	N/A

A10.2	Gestión de la prestación de los servicios por terceras partes.			
A10.2.1	Prestación del servicio.	Se debe garantizar que los controles de seguridad, las definiciones del servicio y los niveles de prestación del servicio incluidos en el acuerdo, sean implementados, mantenidos y operados por las terceras partes.	SI	N/A
A10.2.2	Monitoreo y revisión de los servicios por terceras partes.	Los servicios, reportes y registros suministrados por terceras partes se deben controlar y revisar con regularidad y las auditorias se deben llevar a cabo a intervalos regulares.	NO	
A10.2.3	Gestión de los cambios en los servicios por terceras partes.	Los cambios de la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas existentes de seguridad de la información, en los procedimientos y controles se deben gestionar teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la	NO	N/A

		revaluación de los riesgos.		
A10.3	Protección contra códigos maliciosos y móviles.			
A10.3.1	Gestión de la capacidad.	Se debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.	SI	Se debe especificar las adquisiciones según la necesidad.
A10.3.2	Aceptación del sistema.	Se deben establecer criterios de aceptación para Sistemas de Información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.	SI	Se deben verificar los sistemas adquiridos o modificados.
A10.4	Protección contra códigos maliciosos y móviles.			
A10.4.1	Controles contra códigos maliciosos.	Se debe implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos adecuados de concientización de los	SI	No hay protección continua y completa ante código malicioso.

		usuarios.		
A10.4.2	Controles contra códigos móviles.	Cuando se autoriza la utilización de códigos móviles, la configuración debe asegurar que dichos códigos operan de acuerdo con la política de seguridad claramente definida, y se debe evitar la ejecución de los códigos móviles no autorizados.	NO	No contamos con códigos móviles.
A10.5	Respaldo			
A10.5.1	Respaldo de la información.	Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.	SI	No hay un sistema de backups aprobado ni contínuo.
A10.6	Gestión de la seguridad de las redes			
A10.6.1	Controles de la redes.	Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.	SI	Establecer controles claros de las redes.
A10.6.2	Seguridad de los	En cualquier acuerdo sobre los	SI	Establecer acuerdos

	servicios de la red.	servicios de la red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios que se prestan en la organización o se contratan externamente.		de uso de la red.
A10.7	Manejo de los Medios.			
A10.7.1	Gestión de los medios removibles.	Se deben establecer procedimientos para la gestión de medios removibles.	SI	No hay controles para removibles.
A10.7.2	Eliminación de los medios.	Cuando ya no se requieran estos medios, su eliminación se debe hacer en forma segura y sin riesgo, utilizando los procedimientos formales.	SI	Controlar la eliminación de medios.
A10.7.3	Procedimientos para el manejo de la información.	Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.	SI	Establecer controles para la información que es de carácter privado o de uso exclusivo.
A10.7.4	Seguridad de la documentación del	La documentación del sistema debe estar protegida contra	SI	Es importante proteger la

	sistema.	acceso no autorizado.		documentación del sistema.
A10.8	Intercambio de la información.			
A10.8.1	Políticas y procedimientos para el intercambio de información.	Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación.	NO	N/A
A10.8.2	Acuerdos para el intercambio.	Se deben establecer acuerdos para el intercambio de la información y el software entre la organización y partes externas.	NO	N/A
A10.8.3	Medios físicos en tránsito.	Los medios que contienen información se deben proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la organización.	NO	N/A
A10.8.4	Mensajería electrónica.	La información contenida en la mensajería electrónica debe tener la protección adecuada.	NO	No se utilizan correos corporativos.
A10.8.5	Sistemas de Información del negocio.	Se deben establecer, desarrollar e implementar políticas y procedimientos para proteger la información asociada con la	NO	N/A

		interconexión de los Sistemas de Información del negocio.		
A10.9	Servicios de comercio electrónico.			
A10.9.1	Comercio electrónico.	La información involucrada en el comercio electrónico que se transmite por las redes públicas debe estar protegida contra actividades fraudulentas, disputas de contratos y divulgación o modificación no autorizada.	NO	No se cuenta con servicio comercio electrónico
A10.9.2	Transacciones en línea.	La información involucrada en las transacciones en línea debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración, divulgación, duplicación o repetición no autorizada del mensaje.	SI	En los sistemas en línea se deben verificar las transacciones.
A10.9.3	Información disponible al público.	La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no autorizada.	SI	No hay controles adecuados para los accesos en línea.
A10.10	Monitoreo			
A10.10.1	Registro de	Se debe elaborar y mantener	SI	Documentar las

	auditorías.	durante un periodo acordado las grabaciones de los registros para auditoria de las actividades de los usuarios, la excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.		auditorías.
A10.10.2	Monitoreo del uso del sistema.	Se deben establecer procedimientos para el monitoreo de uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deben revisar con regularidad.	SI	No hay disponible ningún monitoreo actualmente.
A10.10.3	Protección de la información del registro.	Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados.	SI	No hay disponible ningún monitoreo actualmente.
A10.10.4	Registros del administrador y del operador.	Se deben registrar las actividades tanto del operador como del administrador del sistema.	SI	No se controla actualmente
A10.10.5	Registros de falla.	Las fallas se deben registrar y analizar, y se deben tomar las acciones adecuadas.	SI	No hay ningún registro de anomalías detectadas o resultantes.

A10.10.6	Sincronización de relojes.	Los relojes de todos los sistemas de procesamiento de información pertinente dentro de la organización o del dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta y acordada.	SI	No hay ninguna sincronización.
A11	CONTROL DE ACCESO			
A11.1	Requisitos del negocio para el control de acceso.			
A11.1.1	Política de control de acceso.	Se debe establecer, documentar y revisar la política de control de acceso con base a los requisitos del negocio y de la seguridad para el acceso.	SI	No hay políticas de control de acceso.
A11.2	Gestión del acceso de usuarios.			
A11.2.1	Registro de usuarios.	Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.	SI	No hay ningún registro físico de usuarios.
A11.2.2	Gestión de privilegios.	Se debe restringir y controlar la asignación y uso de privilegios.	SI	Existen varias cuentas de admin,

				se deben controlar.
A11.2.3	Gestión de contraseñas para usuarios.	La asignación de contraseñas se debe controlar a través de un proceso formal de gestión.	SI	No hay control ni gestión de contraseñas para el software actual.
A11.2.4	Revisión de los derechos de acceso de los usuarios.	La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.	SI	Controlar los derechos de cada usuario.
A11.3	Responsabilidades de los usuarios			
A11.3.1	Uso de contraseñas.	Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas.	SI	No diferencian actualmente las contraseñas fuertes y débiles.
A11.3.2	Equipo de usuario desatendido.	Los usuarios deben asegurarse de que los equipos desatendidos se les da la protección adecuada.	SI	Todo equipo se debe proteger.
A11.3.3	Política de escritorio despejado y pantalla despejada.	Se debe adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.	SI	No existen políticas para el tema.

A11.4	Control de acceso a las redes			
A11.4.1	Política de uso de servicios de red.	Los usuarios solo deben tener acceso a los servicios para cuyo uso están específicamente autorizados.	SI	Debe existir control de usuarios y roles.
A11.4.2	Autenticación de usuarios para conexiones externas.	Se deben emplear métodos adecuados de autenticación para controlar el acceso de usuarios remotos.	SI	Controlar el acceso remoto.
A11.4.3	Identificación de los equipos en las redes.	La identificación automática de los equipos se debe considerar un medio para autenticar conexiones de equipos y ubicaciones específicas.	SI	Establecer mecanismos de identificación de equipos en la red.
A11.4.4	Protección de los puestos de configuración y diagnostico remoto.	El acceso lógico y físico a los puertos de configuración y de diagnóstico debe estar controlado.	SI	Establecer mejores controles para el uso de puertos.
A11.4.5	Separación de las redes.	En las redes se deben separar los grupos de servicios de información, usuarios y Sistemas de Información.	NO	N/A
A11.4.6	Control de conexión a las redes.	Para redes compartidas, especialmente para aquellas que se extienden más allá de las	SI	Especificar los controles para el uso de las redes

		fronteras de la organización, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control de acceso y los requisitos de aplicación del negocio (véase el numeral 11.1)		compartidas.
A11.4.7	Control de enrutamiento en la red.	Se deben implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control del acceso a de las aplicaciones.	SI	Establecer los controles adecuados para enrutamiento.
A11.5	Control de acceso al sistema operativo.			
A11.5.1	Procedimientos de ingreso seguro.	El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de inicio seguro.	SI	No existen controles para el ingreso a los sistemas operativos.
A11.5.2	Identificación y autenticación de usuarios.	Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un	SI	No hay métodos de identificación de usuarios distintos al logueo normal.

		usuario.		
A11.5.3	Sistema de gestión de contraseñas.	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	SI	Las contraseñas actuales son diseñadas por los mismos usuarios sin control.
A11.5.4	Uso de las utilidades del sistema.	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.	SI	Prohibir el uso de software pirata y controlar el software legal.
A11.5.5	Tiempo de inactividad de la sesión.	Las sesiones inactivas se deben suspender después de un periodo de inactividad.	SI	No existe un buen control de sesiones.
A11.5.6	Limitación del tiempo de conexión.	Se deben utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo.	SI	Establecer un control con el tiempo de cada conexión, especialmente porque no lo hay.
A11.6	Control de acceso a las aplicaciones y a la información.			
A11.6.1	Restricciones de acceso a la información.	Se debe restringir el acceso a la información y las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida en el control de	SI	Las bases de datos de la institución no tienen controles adecuados.

		acceso.		
A11.6.2	Aislamiento de sistemas sensibles.	Los sistemas sensibles deben tener un entorno informático dedicado (aislados).	SI	No hay sitios dedicados para los sistemas sensibles.
A11.7	Computación móvil y trabajo remoto.			
A11.7.1	Computación y comunicaciones móviles.	Se debe establecer una política formal y se deben adoptar las medidas de seguridad apropiadas para la protección contra riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.	SI	No hay actualmente controles ni políticas de seguridad para dispositivos móviles.
A11.7.2	Trabajo remoto.	Se deben desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.	NO	N/A
A12	ADQUISICION, MANTENIMIENTO Y DESARROLLO DE MANTENIMIENTOS DE INFORMACION.			
A12.1	Requisitos de Seguridad de los Sistemas de Información.			
A12.1.1	Análisis y especificación de	Las declaraciones sobre los requisitos del negocio para	SI	Crear controles para nuevos Sistemas de

	los requisitos de seguridad.	nuevos Sistemas de Información o mejoras de los sistemas existentes deben especificar los requisitos para los controles de seguridad.		Información.
A12.2	Procesamiento correcto de las aplicaciones.			
12.2.1	Validación de los datos de entrada.	Se deben validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados.	SI	Crear un sistema de validación de datos.
12.2.2	Control de procesamiento interno.	Se deben incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados.	SI	Crear los controles necesarios.
12.2.3	Integridad del mensaje.	Se deben identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.	NO	No se requiere integridad de los mensajes
12.2.4	Validación de los datos de salida.	Se deben validar los datos de salida de una aplicación para	NO	N/A

		asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias.		
A12.3	Controles Criptográficos.			
12.3.1	Política sobre el uso de controles criptográficos.	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	SI	Actualmente no hay ningún control criptográfico.
12.3.2	Gestión de llaves.	Se debe implementar un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas por parte de la organización.	NO	No se va a implementar llaves criptográficas.
A12.4	Seguridad de los archivos del sistema.			
12.4.1	Control del software operativo.	Se deben implementar procedimientos para controlar la instalación de software en los sistemas operativos.	SI	Controlar toda instalación de software en los sistemas operativos de los servidores.
12.4.2	Protección de los datos de prueba del sistema.	Los datos de prueba deben seleccionarse cuidadosamente, así como protegerse y controlarse.	NO	No se usan datos de prueba.

12.4.3	Control de acceso al código fuente de los programas.	Se debe restringir el acceso al código fuente de los programas.	NO	No se maneja código fuente de ningún programa.
A12.5	Seguridad en los procesos de desarrollo y soporte			
12.5.1	Procedimientos de control de cambios.	Se debe controlar la implementación de cambios utilizando procedimientos formales de control de cambios.	SI	Establecer controles para los cambios en hardware y software.
12.5.2	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo.	Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.	SI	En situaciones de cambio del sistema operativo.
12.5.3	Restricciones en los cambios a los paquetes del software.	Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	SI	Controlar los cambios de versiones y actualizaciones.
12.5.4	Fuga de información.	Se debe evitar las oportunidades para que se produzca fuga de información.	SI	Establecer controles estrictos para evitar estos problemas.

12.5.5	Desarrollo de software contratado externamente.	La organización debe supervisar y monitorear el desarrollo de software contratado externamente.	SI	Cuando se contrate con terceros la creación de software.
A12.6	Gestión de la vulnerabilidad técnica.			
12.6.1	Control de vulnerabilidades técnicas.	Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los Sistemas de Información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.	SI	Analizar y evaluar los riesgos para minimizar o quitar las vulnerabilidades y amenazas.
A13	GESTION DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACION.			
A13.1	Reporte sobre los eventos y las debilidades de la seguridad de la información.			
13.1.1	Reporte sobre los eventos de seguridad de la información.	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.	SI	Establecer los canales de comunicación.

13.1.2	Reporte sobre las debilidades de la seguridad.	Se debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.	SI	Comunicar y reportar fallas.
13.2	Gestión de los incidentes y las mejoras en la seguridad de la información.			
13.2.1	Responsabilidades y procedimientos.	Se deben establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	SI	Crear los procedimientos para los incidentes.
13.2.2	Aprendizaje debido a los incidentes de seguridad de la información.	Deben existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.	SI	No existen controles de los incidentes de seguridad ocurridos.
13.2.3	Recolección de evidencia.	Cuando una acción de seguimiento contra una persona u organización después de un	NO	N/A

		incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.		
A14	GESTION DE LA CONTINUIDAD DEL NEGOCIO			
A14.1	Aspectos de seguridad de la información, de la gestión de la continuidad del negocio.			
14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	Se debe desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.	SI	La continuidad del negocio es uno de los fines del SGSI.
14.1.2	Continuidad del negocio y evaluación de riesgos.	Se debe identificar los eventos que puedan ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de	SI	Adecuada gestión de riesgos.

		dichas interrupciones, así como sus consecuencias para la seguridad de la información.		
14.1.3	Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información.	Se deben desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos críticos para el negocio.	SI	Crear los planes de recuperación.
14.1.4	Estructura para la planificación de la continuidad del negocio.	Se debe mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento.	SI	Crear los planes de continuidad del negocio.
14.1.5	Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio.	Los planes de continuidad del negocio se deben someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.	SI	Revisión de los planes de continuidad.

A15	CUMPLIMIENTO			
A15.1	Cumplimiento de los requisitos legales.			
15.1.1	Identificación de la legislación aplicable.	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada Sistema de Información y para la organización.	SI	Aplicar la legislación colombiana.
15.1.2	Derechos de la propiedad intelectual (DPI).	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.	SI	Establecer normas solo para usar software licenciado.
15.1.3	Protección de los registros de la organización.	Los registros importantes se deben proteger contra perdida, destrucción y falsificación, de acuerdo con los requisitos	SI	Proteger los registros.

		estatutarios, reglamentarios, contractuales y del negocio.		
15.1.4	Protección de los datos y privacidad de la información personal.	Se debe garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes, si se aplica, con las cláusulas del contrato.	SI	Establecer controles para proteger los datos y la privacidad de cierta información.
15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información.	Se debe disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.	SI	Controlar el uso no autorizado de procesamiento de la información.
15.1.6	Reglamentación de los controles criptográficos.	Se deben utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.	SI	No hay ningún control hasta el momento.
A15.2	Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico.			
15.2.1	Cumplimiento con las políticas y normas de seguridad.	Los directores deben garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr	SI	Verificar el cumplimiento de las políticas de seguridad.

		los cumplimientos con las políticas y las normas de seguridad.		
15.2.2	Verificación del cumplimiento técnico.	Los Sistemas de Información se deben verificar periódicamente para verificar el cumplimiento con las normas de implementación de la seguridad.	SI	Verificar el cumplimiento de las políticas de seguridad.
A15.3	Consideraciones de la auditoria de los Sistemas de Información.			
15.3.1	Controles de auditoria de Los Sistemas de Información.	Los requisitos y las actividades de auditoria que implican verificaciones de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.	SI	Crear controles de auditorías.
15.3.2	Protección de las herramientas de auditoria de los Sistemas de Información.	Se debe proteger el acceso a las herramientas de auditoria de los Sistemas de Información para evitar su uso inadecuado o ponerlas en peligro	SI	Las herramientas de auditoría se deben proteger.

Fuente: Anexo A ISO 27001-Autor.

18. PLAN DE TRATAMIENTO DEL RIESGO

El objetivo primordial es el de establecer responsabilidades sobre la aplicación de la declaración de aplicabilidad del SGSI, definiendo además las medidas necesarias para mitigar o minimizar el riesgo.

18.1 ROLES Y RESPONSABILIDADES RELACIONADOS CON SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es un área amplia que afecta a toda la institución educativa Luis Carlos Galán, por esta razón se hace necesario describir los roles y responsabilidades que se relacionan a continuación:

Tabla 34. Definición de roles y responsabilidades

ROL	RESPONSABILIDAD
Dirección general (Rector y Consejo Directivo)	• Establece la política del SGSI. • Se asegura que se establezcan los objetivos y planes del SGSI. • Establece funciones y responsabilidades de seguridad de la información. • Asegura la integración de los requisitos del SGSI en los procesos de la organización. • Asegurar que el SGSI logre los resultados previstos. • Dirige y apoya a las personas, para contribuir a la eficacia del SGSI. • Apoya otros roles para demostrar liderazgo aplicado a sus áreas de responsabilidad. • Establece y mantiene un compromiso con el proceso de medición. • Comunica la importancia de cumplir los objetivos de seguridad de la información de conformidad con la política, responsabilidades de ley y mejora continua. • Responsable de la visión, toma de decisiones estratégicas y coordinación de las actividades para dirigir y controlar la organización. • Aprueba la política de gestión de incidentes de seguridad de la información. • Provee los recursos suficientes para establecer, implementar, operar, hacer seguimiento, revisar,

	mantener y mejorar el SGSI. • Decidir sobre los criterios de aceptación y niveles de riesgos. • Asegurarse que se efectúan auditorías internas de SGSI. • Garantiza que la seguridad de la información se aborde adecuadamente en toda la organización. • Compromiso con el esquema de gestión de incidentes de seguridad de la información. • Efectuar revisión por la dirección del SGSI.
Jefe de seguridad de la información (Actual jefe de sistemas)	• Responsabilidad y gobierno de la seguridad de la información, que asegura el manejo correcto de los activos de información. • Asesora al equipo de la alta dirección, proporciona soporte especializado al personal de la organización y asegura que los límites del estado de seguridad de la información estén disponibles. • Asegura el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios. • Asegura que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.
Parte involucrada	• En el contexto de las descripciones de otros roles acerca de seguridad de la información, la parte involucrada se define aquí principalmente como las personas por fuera de las operaciones normales, tales como la junta directiva, estudiantes, padres de familia, proveedores y entidades públicas relacionadas con la educación en Colombia.
Seguridad física (Celadores)	• Responsable de la seguridad física e instalaciones. • 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.

18.2 LISTADO DE PROCEDIMIENTOS PREVENTIVOS

Con el fin de buscar reducir el riesgo, se hacen algunas recomendaciones para la institución educativa.

1. No ubicar ni almacenar cerca de elementos inflamables como papel, gasolina, ether, bebidas alcohólicas, alcohol, trapos.

2. Se debe garantizar una temperatura adecuada para el buen funcionamiento del equipo. La temperatura será especificada de acuerdo al dispositivo e indicada en el manual del respectivo elemento.

3. La ubicación de los equipos debe ser preferiblemente en lugares donde existan paredes de concreto.

4. No se deben ubicar papeleras de basura en los recintos destinados como cuartos de telecomunicaciones, ya que se pueden convertir en yesca de un posible incendio.

5. El personal que tiene a cargo la administración de la red, debe tener claro los tipos de incendio que se pueden presentar y diseñar los controles tanto preventivo como correctivo para cada caso.

6. Se deben tener extintores de polvo químico seco y de bióxido de carbono en lugares visibles y cercanos a donde se encuentran ubicados los equipos.

7. Se debe capacitar al personal sobre el manejo de los diferentes extintores con que se cuenta.

8. Dar el adecuado uso a los diferentes elementos evitando siempre prácticas inseguras.

9. No fumar en lugares donde se concentra los equipos como centro de cómputos, cuarto de comunicaciones.

10. Nunca consumir alimentos ni ingerir bebidas cerca de los equipos.

11. No manipule equipos en estado de embriaguez ni bajo efecto de sustancias alucinógenas.

12. Controlar el acceso de paquetes al centro de cómputo y cuarto de comunicaciones.

13. Tener una excelente distribución eléctrica, evitando conectar los equipos a una misma fuente.

14. Evitar extensiones y cables sueltos cerca a los equipos.

15. Instalar alarmas de activación manual o automáticas en caso de presentarse incendio, inundación, sobrecalentamiento de equipos.

16. Evitar la acumulación de la energía estática referenciando todos los equipos a una misma tierra.

17. Todos los equipos deben tener protección contra cortocircuitos y sobrevoltaje ya sea interna o externa.

18. Tener pólizas de seguros vigentes de los elementos que conforman la red corporativa.

19. No ubicar aparatos eléctricos dentro del centro de cómputo y cuarto de comunicaciones tales como grabadoras, hornos microondas, licuadoras, televisores y demás.

19. Verificar diariamente el correcto funcionamiento de las lámparas y tomacorrientes ubicados en el centro de cómputo.

21. Colocar los equipos en un cuarto de telecomunicaciones o centro de cómputo, donde se concentre la mayoría de equipos de comunicaciones.

22. La ubicación debe ser en un sitio interior, de alta seguridad, no tener ventanales y no existir tuberías alrededor.

23. Los equipos sólo debe ser manipulados por el personal que tenga los suficientes conocimientos acerca de ellos.

24. Permitir solo el acceso de personas que realicen labores de operación y mantenimiento de los equipos.

25. Mantener información en archivos e impresa de los proveedores y garantías vigentes de todos los equipos utilizados en la red.

26. Tener información actualizada de las diferentes empresas que prestan servicios de soporte y mantenimiento de los equipos.

27. Realizar un contrato y mantenerlo vigente con una empresa prestadora del servicio de soporte y mantenimiento en redes de datos.

28. Comprar seguros a los equipos de la red, que cubran daños, actos mal intencionados, hurto.

29. Guardar en un archivo tanto dentro como fuera de la institución educativa la información sobre la configuración inicial de todos los equipos.

30. Destinar un sitio seguro y de acceso restringido para guardar manuales, software de instalación (Cds, Diskettes), documentación de los equipos, ejerciendo un estricto control sobre su uso.

31. Tener copia de cada uno de los manuales y software, evitando al máximo el uso de originales.

32. No se debe tener más del 20% del tráfico sostenido por segmento, este número podría disminuir de acuerdo al tipo de aplicaciones que se manejen en el segmento.

33. Capacitar continuamente al personal de sistemas en temas de relacionados con tecnología de punta.

34. Tener un sistema de energía regulada alterno que entre a operar en el momento que falle el suministro actual.

40. Cualquier falla en el hardware ó software llamar inmediatamente al proveedor o a la empresa que tenga en el momento de la ocurrencia el contrato de mantenimiento de la red, o también llevar a cabo el procedimiento de reparación y/o reemplazo.

19. AUDITORÍA INTERNA

19.1 OBJETIVO DE LA AUDITORÍA INTERNA

Verificar el funcionamiento del Sistema de Gestión de Seguridad de Información de la Institución Educativa Luis Carlos Galán para verificar si los controles, procesos y procedimientos están acorde a la norma.

19.2 FORMATO INICIAL DE AUDITORÍA

El formato pretende verificar si los controles se están llevando a cabo según el SGSI a cargo del responsable, además verificar su indicador con el propósito de saber hasta qué porcentaje ha sido verificado para evaluar la efectividad y comparar entre el estado inicial y el actual.

Tabla 35. Formato plan de auditoría

HALLAZGOS DE AUDITORÍA				
ID	**Hallazgo**	**Numeral de la Norma**	**Descripción**	**Tipo de Hallazgo**

Fuente: Autor

Posteriormente y según los resultados encontrados con los procesos del SGSI, si algunos de estos no se cumplen tanto completamente como parcialmente, se debe redactar el registro de no conformidades para generar mejoras.

19.3 ALCANCE DE LA AUDITORÍA

Constatar las acciones tomadas, mantener disponible y en funcionamiento eficiente cada componente del SGSI, todo dentro de la misma organización, defendiendo las políticas y objetivos planteados.

19.4 PERIODICIDAD

Se debe realizar una auditoría interna cada seis (6) meses, un mes antes de la auditoría se debe informar por escrito a los entes involucrados en la institución para informar y recordar la ejecución de la auditoría.

19.5 AUDITORES

Previamente se debe elegir al equipo auditor conformado mínimo por un profesional en sistemas de la misma institución educativa o externo y delegados o representante de las directivas de la institución.

19.6 SEGUIMIENTO A LA AUDITORÍA

Se debe hacer el respectivo seguimiento de la auditoría documentando todo el proceso para buscar mejorar el mismo.

19.7 METODOLOGIA Y CRITERIOS DE AUDITORIA

En el proceso de consolidación de la información para realizar el proceso de la auditoría se realizan las siguientes actividades in situ según la norma ISO 27001:2013:

- Realización de la reunión de apertura. Es importante este espacio para dar claridad al objetivo, alcance y criterios de la auditoria.
- Comunicación durante la auditoria

- Recopilación y verificación de la información
- Generación de hallazgos de la auditoria
- Realización de la reunión de cierre. Es importante este espacio para dar a conocer a la gerencia y dueños de proceso las fortalezas, observaciones y oportunidades de mejora del SGSI, para aprobar el informe de auditoría.
- Seguimiento y revisión del programa: Se identifican acciones preventivas y correctivas y oportunidades de mejora del sistema de seguridad de la información.
- Se establece la mejora del programa de auditoría.

19.8 Resultados auditoria interna

A continuación un resumen de la autoría efectuada por un ingeniero externo a la institución.

HALLAZGOS DE AUDITORÍA				
ID	**Hallazgo**	**Numeral de la Norma**	**Descripción**	**Tipo de Hallazgo**
1	Contacto con las autoridades	A.6.1.3	No se encuentra evidencia suficiente de que exista un contacto con las autoridades ni procedimientos que especifiquen en qué momento y quién debe contactar a las autoridades y cómo deben ser reportados los incidentes de seguridad a tiempo.	**No Conformidad Menor**
2	Gestión de derechos de acceso privilegiado	A.9.2.3	Se hace bajo demanda, pero aún falta documentar y mejorar las restricciones y privilegios en algunos servicios como Sigedin Académico.	**No Conformidad Menor**
3	Revisión de los derechos de acceso de usuarios	A.9.2.5	No se ha contemplado en ninguna política la revisión de los derechos de acceso de manera periódica, esto debe ser definido e implementado. Puede considerarse la inclusión de este control dentro de la política de control de acceso que está planeada para ser implementada.	**No Conformidad Menor**
4	Conexiones seguras	A.6.1.4	Se puede apreciar que aún falta mejorar las conexiones seguras con servidores locales y web institucional para los diferentes servicios.	**Oportunidad de Mejora**
5	Inventario de Activos	A.8.1.1	Este control se aplica de manera intuitiva sin embargo es recomendable que se establezca un procedimiento para que sea repetible, se pueda gestionar y medir y posiblemente posteriormente automatizar.	**Oportunidad de Mejora**
6	Uso de información de autenticación secreta	A.9.3.1	Para lograr aumentar el nivel de madurez de este control se recomienda incluirlo en una política específica y dentro del temario de concienciación y capacitación.	**Oportunidad de Mejora**
7	Procedimiento de ingreso seguro	A.9.4.2	Se recomienda implementar un procedimiento que permita medir y mejorar este control.	**Oportunidad de Mejora**
8	Uso de programas utilitarios privilegiados	A.9.4.4	La revisión y gestión de la consola centralizada del antivirus se hace solamente por demanda y a criterio del administrador, es aconsejable madurar este control por medio de un procedimiento y guías de revisión y gestión de la consola de antivirus u otras herramientas de apoyo.	**Oportunidad de Mejora**

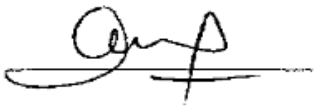
9	Protección contra las amenazas externas y ambientales	A.11.1.4	Se ha implementado este control por demanda, sin embargo no hay una revisión periódica ni se encuentra definido formalmente.	**Oportunidad de Mejora**
10	Servicios de suministro	A.11.2.2	Se cuenta con UPS suficientes para dar autonomía a los servidores así como redes reguladas de energía. Sin embargo no está definido formalmente el mantenimiento y gestión de estos equipos.	**Oportunidad de Mejora**
11	Disposición segura o reutilización de equipos	A.11.2.7	El área de tecnología tiene la costumbre de hacer un borrado a bajo nivel de los discos duros de equipos de personal que se retira de la compañía o en el caso de reasignación de equipos. Sin embargo no está formalizado.	**Oportunidad de Mejora**
12	Planificación de la continuidad de la seguridad de la información	A.17.1.1	La organización tiene desarrollado un Plan de continuidad de negocio en donde tiene en cuenta ciertos controles de seguridad de acuerdo con el criterio del área de tecnología.	**Oportunidad de Mejora**

CONCLUSIONES

Se logra apreciar que no se encontraron conformidades mayores, se encontraron 3 conformidades menores y 9 oportunidades de mejora.

Como observación general debe decirse que debido al estado inicial del SGSI, el 70% de los controles de la norma se encuentran en estado de implementación dentro de lo establecido por el mismo SGSI y en su plan de tratamiento de Riesgos, en esta auditoría inicial no se catalogan como no conformidades pero debe tenerse en cuenta que en futuras auditorías al sistema se espera que el nivel de madurez de dichos controles ya haya aumentado.

Haciendo una comparación entre el estado inicial (antes del SGSI) y el estado actual, se puede deducir que la seguridad de la información ha aumentado significativamente, pues la mayor parte de los controles y políticas se encuentran implementadas y se cumplen por parte del personal de la institución.



Ing. JHONY RICARDO CERON CHAVEZ
Mg. En Software Libre
Esp. Auditoria de Sistemas
Cel. 3115816325

20. CONCLUSIONES

- En la sociedad de información que se vive actualmente, es conveniente que toda empresa u organización de cualquier carácter o tamaño implemente mecanismos de seguridad, teniendo en cuenta la normatividad existente como la ISO/IEC 27001:2013 para buscar problemas de seguridad y establecer los controles necesarios para salvaguardar la información.

- Existen normas y metodologías como Magerit en el ambiente de seguridad, que permiten hacer análisis y estimación del riesgo de forma ordenada y sistemática para obtener resultados que ayudan de forma eficaz en el SGSI.

- La institución educativa Luis Carlos Galán no contaba con mecanismos de control de seguridad de su información, por tal motivo la elaboración del SGSI para su implementación permite dar un paso importante para salvaguardar su activo más importante.

- A través del desarrollo del presente proyecto, se da cumplimiento a los objetivos propuestos en pro de la seguridad, con la participación y compromiso de todos para el fiel cumplimiento de las políticas propuestas en el plan.

- El análisis de riesgos permite conocer de forma eficiente y veraz el estado actual de la seguridad informática en la institución educativa Luis Carlos Galán, como un baluarte para proceder con la metodología y saber de qué manera podemos tener problemas de seguridad.

- Con el análisis de riesgos, se lograron establecer controles y políticas establecidos en el presente sistema de gestión de seguridad de la información, encaminado a optimizar los objetivos de la institución educativa, incrementar la confiabilidad, integridad y disponibilidad de la información.

- La institución educativa Luis Carlos Galán presenta actualmente un nivel considerable de riesgo informático, pero con el apoyo de las directivas y de todo el personal es posible contrarrestar.

BIBLIOGRAFÍA

CABALLERO QUESADA Alonso Eduardo (2013). Manual de pruebas y Hacking con Kali Linux. {10 de Febrero de 2015}. {En línea}. Disponible en: (http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf).

DOCUMENTACIÓN OFICIAL DEL SOFTWARE KALI LINUX, {20 de Febrero de 2015}. {En línea}. Disponible en: (http://www.kali.org/official-documentation).

GUERRÓN JORGE.. (2013). Elaboración de un plan para la implementación del sistema de gestión de seguridad de la información. Lonja. {12 de Febrero de 2015}. {En línea}. Disponible en: (http://openaccess.uoc.edu/webapps/o2/bitstream/10609/19067/24/jguerronTFM0113memoria.pdf).

HERRAMIENTAS, web destinada a gestión de programas en seguridad de la información. {10 de Marzo de 2015}. {En línea}. Disponible en: (http://www.iso27000.es/herramientas.html).

ARQUEZ DE MELO, José “Comunicación e integración latinoamericana: El papel de ALAIC”. {En línea}. {10 julio de 2015} disponible en: (www.mty.itsem.mx/externos/alaic/texto1html).

METODOLOGÍA MAGERIT Y ANEXOS, herramienta PILAR. {12 de Marzo de 2015}. {En línea}. {10 de Marzo de 2015} disponible en: (https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/).

MINTIC GOBIERNO DE COLOMBIA. “Ley 1273 de 2009 delitos informáticos”. {En línea}. {10 de Marzo de 2015} disponible en: (http://www.mintic.gov.co/portal/604/w3-article-3705.html).

MONJE C. (2011). Metodología de la investigación cuantitativa y cualitativa. Guía didáctica. {En línea}. {15 de Marzo de 2015}. disponible en: (http://carmonje.wikispaces.com/file/view/Monje+Carlos+Arturo++Gu%C3%ADa+did%C3%A1ctica+Metodolog%C3%ADa+de+la+investigaci%C3%B3n.pdf).

PALLAS MEGA GUSTAVO. (2009), Metodología de implantación de un SGSI en un grupo empresarial jerárquico, Universidad de la República, Montevideo Uruguay. {En línea}. {15 de Marzo de 2015} disponible en: (http://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf).

POLÍTICAS GOBIERNO DE COLOMBIA EN SGSI PARA ENTIDADES PÚBLICAS {En línea}. {20 de Marzo de 2015} disponible en: (http://www.mintic.gov.co/gestionti/615/w3-channel.html).

UNIVERSIDAD NACIONAL DE COLOMBIA.. (2007). Indicaciones para elaborar la propuesta para trabajo de grado. {En línea}. {22 de Marzo de 2015} disponible en: (http://www.docentes.unal.edu.co/flozanoo/docs/INDICACIONES%20PARA%20ELABORAR%20LA%20PROPUESTA.ppt.).

21. ANEXOS

21.1 AUTORIZACIÓN POR PARTE DE LA INSTITUCIÓN

Figura 6. Autorización de la institución

REPUBLICA DE COLOMBIA
MUNICIPIO DE VILLAGARZON
DEPARTAMENTO DEL PUTUMAYO
Institución Educativa "Luis Carlos Galán"
Aprobado mediante Decreto de Fusión N° 062 del 06/12/2002
"Siempre adelante, ni un paso atrás"

Villagarzón, 5 de Febrero de 2015

AUTORIZACIÓN

Por medio de la presente y después de analizar la propuesta de tesis de grado para optar el título de Especialista en Seguridad Informática de la UNAD y relacionada con la creación de un Sistema de Gestión de Seguridad Informática para la Institución Educativa Luis Carlos Galán, nos permitimos **AUTORIZAR** su elaboración e implantación de este trabajo al Ingeniero JAIRO HERNANDO QUINTERO MADROÑERO, identificado con cédula No. 18102921, quien actualmente labora en esta misma institución y es el encargado de la parte de Sistemas en la misma.

Así mismo la parte directiva autoriza para que el ingeniero Jairo sea quien esté al frente del proyecto, contando con nuestro decidido respaldo y apoyo económico por parte de la institución, para los cambios que sean convenientes o capacitaciones al personal, con el objeto de mejorar la seguridad informática del colegio y prevenir problemas futuros.

Cabe resaltar que este proyecto redundará en beneficio general a la protección de la información institucional, situación que ha sido hasta el momento preocupación de todos para prestar normalmente los servicios a la comunidad educativa.

Cordialmente,

Esp. SEGUNDO MAURO VELASQUEZ BENAVIDES
C.C. No. 18100516
Rector I. E. LUIS CARLOS GALÁN

Carrera 1 No. 1-48 – Barrio Obrero Villagarzón Putumayo
Web: www.colegiogalanvilla.edu.co – Correo: colgalanvivet@hotmail.com

Fuente: autor

21.2 HOJA DE VIDA DE EQUIPOS DE CÓMPUTO

Cada computador tener una hoja de vida con el formato que se describe a continuación, con el objeto de hacer seguimiento a su funcionamiento y revisiones o cambios tanto en hardware como en software.

OBSERVACIÓN: Si es un computador portátil de dejan en blanco algunos cuadros que no aplican.

DATOS BÁSICOS

Tabla 36. Formato de Hoja de vida de computador

No. Interno		**MARCA**			**Marca monitor**			
Referencia			**Serial**		**Ref. monitor**		**Serial Monitor**	
Board			**Serial Board**		**Teclado**		**Serial teclado**	
Procesador		**Velocidad GHz**	**Serial proc.**		**Mouse**		**Serial mouse**	
Memoria RAM		**Capacidad Mb**	**Serial RAM**		**CDROM**		**Serial CDROM**	
Disco Duro marca		**Capacidad Gb**	**Serial**		**Unidad de DVD**		**Serial DVD**	
			Tipo		**Lector Multitarjetas**		**Serial**	
Tarjeta de video		**Capacidad Mb**	**Serial video**		**Otros**		**Serial**	
Tarjeta de sonido			**Serial sonido**		**Otros**		**Serial**	

SOFTWARE

Sistema operativo Versión		Service pack		Licencias	SI	NO
Paquete office		Service pack		Otros		
Navegadores		Otros		Otros		
Multimedia						
Otros programas						

SEGUIMIENTO DE MANTENIMIENTO

N°	DESCRIPCIÓN								FECHA	
1.	Tipo mantenimiento :	Preventivo		Correctivo		Predictivo			Fecha y hora de Entrada	
	Trabajos realizados:								Fecha y hora de salida	
2.	Tipo mantenimiento	Preventivo		Correctivo		Predictivo			Fecha y hora de Entrada	
	Trabajos realizados:								Fecha y hora de salida	
3.	Tipo de mantenimiento	Preventivo		Correctivo		Predictivo			Fecha y hora de Entrada	
	Trabajos realizados:								Fecha y hora de salida	

Fuente: Autor

21.3 PROCEDIMIENTO PARA MANTENIMIENTOS

21.3.1 Propósito del mantenimiento. Proporcionar mantenimiento a las instalaciones y equipos para que se conserven en condiciones óptimas de funcionamiento, previniendo las posibles averías y fallos, y consiguiendo así que el trabajo se realice con los mayores niveles de calidad y seguridad. El mantenimiento debe ser aplicado solo por el personal del departamento de informática o terceros debidamente autorizados.

21.3.2 Aplicación. Todas las instalaciones y equipos utilizados por la empresa.

21.3.3 Procedimiento. 1. Los responsables del mantenimiento son el personal del departamento de sistemas, junto con el grupo de colaboradores que esta oficina designe, elaborará un programa de mantenimiento preventivo cuyo propósito es llevar a cabo un buen control de los registros de los equipos en mantenimiento, quienes los solicitan y lo requieren.

2. Cada equipo o conjunto de equipos idénticos dispondrán de una identificación de registro del programa de revisiones a realizar en cada uno de ellos, en el que se recogerán los trabajos de mantenimiento y reparación realizados. Para ello estarán identificados los elementos y las partes críticas de los equipos objeto de revisión y los aspectos concretos a revisar.

3. Se dispondrá de hojas de revisión mediante cuestionarios de chequeo para facilitar el control de los elementos y aspectos a revisar, en donde el personal indicara las actuaciones y desviaciones detectadas de acuerdo con los estándares establecidos. En dichas hojas constaran la frecuencia y la fecha de las revisiones así como los responsables de realizarlas. Las hojas de revisión cumplimentadas, así como los registros de los trabajos realizados, se guardaran en las propias unidades funcionales.

4. Cada mantenimiento preventivo estará debidamente codificado y se

registrara en la hoja destinada nombrada como "*Ficha de mantenimiento y revisión de equipos"*. Se diferenciarán, en función de la frecuencia requerida, las diferentes actuaciones, bien sea de verificación de estándares o bien se trate de tareas específicas.

5. Resultados de las revisiones preventivas: cuando el curso de una revisión se detecten anomalías, estas deberán ser notificadas. Obviamente, siempre que sea posible se repararán inmediatamente o se programará su solución. Estas anomalías encontradas se reflejaran en el formulario destinado de la misma.

6. Independientemente de las actuaciones surgidas de las desviaciones detectadas en el programa de mantenimiento existente una vía de comunicación de cualquier anomalía que el personal detecte en su equipo a través del cumplimiento del formulario o ficha de hoja de vida de cada equipo.

21.4 PROCEDIMIENTO PARA DAR DE BAJA EQUIPOS

Debido a que es una institución educativa de carácter público, es necesario ajustarse a las normas nacionales de Colombia para establecer los mecanismos y procedimiento para dar de baja a elementos devolutivos.

1. Crear una lista de inventario a través de un formato, de los equipos obsoletos o dañados que necesiten ser dados de baja de la Institución Educativa Luis Carlos Galán de Villagarzón Putumayo.

Tabla 37. Formato lista de elementos para dar de baja

No. INTERNO	DETALLE	REFERENCIA	No. SERIAL	ESTADO Obsoleto Dañado
Fecha: Jefe de Sistemas			Fecha: Rector(a)	

Fuente: Autor

2. Visto bueno de la lista de equipos por parte del jefe de sistemas y el señor rector o rectora de la institución, previa revisión de los mismos.
3. Crear una resolución interna para dar de baja los equipos autorizados en el procedimiento anterior.
4. Entregar los equipos en forma de enajenación a título gratuito a otro ente o persona si fuere el caso, de lo contrario entregarlos a alguna empresa encargada del desarme para reciclaje de circuitos y demás partes.

21.5 PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENCIAS, RECLAMARACIONES Y SUGERENCIAS.

21.5.1 Objeto del procedimiento de incidencias. El objeto de este procedimiento es el de establecer la sistemática de reclamaciones, incidencias y sugerencias en los Sistemas de Información de la institución educativa Luis Carlos Galán, aplicado tanto al hardware como al software.

21.5.2 Aplicación del procedimiento de incidencias. Este procedimiento será de aplicación tanto en la gestión como en la revisión del desarrollo de las incidencias, reclamaciones y sugerencias que se formulen derivadas de la actividad en el área de sistemas del colegio.

21.5.3 Definiciones. **INCIDENCIA:** Un incidente de seguridad de la información es un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de cualquier recurso informático; o cualquier otro acto que implique una violación a la Política de Seguridad de la Información de la institución educativa.

QUEJA: Expresión documentada a través de la que se manifiesta disconformidad con un hecho o situación dentro del funcionamiento de los sistemas informáticos de la institución.

RECLAMACIÓN: Oposición o contradicción que se hace a algo como injusto, o mostrar no estar de acuerdo en ello.

SUGERENCIA: Insinuar cambios para la revisión y mejora de cualquier actividad dentro del funcionamiento informático de la institución.

20.6 PROCESO DE RECEPCIÓN Y RESPUESTA

Para toda incidencia, reclamación o sugerencia, se debe reportar por escrito llenando el correspondiente formulario o formato para tal fin, llevarlo y presentarlo

ante la oficina de sistemas de la institución educativa Luis Carlos Galán, en el segundo piso del bloque II.

La oficina de Sistemas tiene un plazo de tres (3) días hábiles para tomar medidas en caso de reclamaciones, dos (2) días hábiles para sugerencias y un plazo máximo de 24 horas para situaciones de incidencias de seguridad para tonar las medidas correspondientes, con el permiso de las directivas para llevar las acciones necesarias con el fin de colocar en estado normal el sistema de hardware o software afectado.

21.7 REVISIÓN Y MEJORA DEL PROCEDIMIENTO

La revisión del procedimiento anterior se hará cada dos (2) años con el propósito de revisar y definir si las respuestas han sido benéficas para el buen funcionamiento o de lo contrario si existen problemas para establecer algunos cambios que ostenten una mejor situación.

21.8 FORMATOS DE REGISTRO

Para presentar una incidencia, reclamación o sugerencia se utiliza el siguiente formato:

Tabla 38. Formato de registro de incidencias y demás

INSTITUCIÓN EDUCATIVA LUIS CARLOS GALÁN VILLAGARZÓN PUTUMAYO FORMULARIO DE REGISTRO			
FECHA:		Incidencia de seguridad	
AREA:		Reclamo	
		Sugerencia	
Descripción:	Escriba con sus palabras la incidencia, reclamo o sugerencia.		
Firma Nombres Identificación Teléfono			