GESTION DE SEGURIDAD DE LA INFORMACION EN LA INSTITUCIÓN EDUCATIVA LEÓN XIII DEL MUNICIPIO DE SOACHA

TRABAJO DE GRADO

JENNY MILENA ROZO CUESTAS

Código 1512011035

OMAR SUAREZ AGUILERA

Código 1512010948

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2016

GESTION DE SEGURIDAD DE LA INFORMACION EN LA INSTITUCIÓN EDUCATIVA LEÓN XIII DEL MUNICIPIO DE SOACHA

TRABAJO DE GRADO

JENNY MILENA ROZO CUESTAS

Código 1512011035

OMAR SUAREZ AGUILERA

Código 1512010948

Asesor

GIOVANNY ANDRES PIEDRAHITA SOLORZANO

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2016

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

Bogotá, Abril 25 de 2016

INTRODUCCION

La institución educativa LEON XIII del municipio de Soacha presenta una problemática en cuanto a la seguridad de los datos que a diario utilizan, desde los archivos de constancias de estudio, bases de datos con la información de cada estudiante hasta el intercambio de información vía correo electrónico entre las instituciones educativas y la secretaria de educación y cultura de Soacha.

Esta información no es respaldada de la forma adecuada poniéndola en peligro de ser borrada, extraída y modificada, además no se tienen establecidos procedimientos que permitan a cada uno de los funcionarios garantizar los pilares de la seguridad de la información Integridad, Disponibilidad, Confidencialidad y no repudio; así como garantizar que los equipos de cómputo donde desarrollan las actividades cuenten con el mínimo de seguridad.

INDICES

pág.

LISTA DE FIGURAS

LISTA DE TABLAS

AGRADECIMIENTOS

Este trabajo de grado está dedicado principalmente a nuestros hijos, quienes han tenido que sacrificar tiempo valioso que antes les ofrecíamos para realizar actividades juntos, por las actividades referentes a esta especialización, lo importante fue que entendieron la importancia de esta superación; a nuestros padres, quienes a pesar de ver nuestros días de cansancio y fatiga, nunca fue impedimento para alentarnos a continuar con el logro de las actividades académicas, siempre atentos a que cumpliéramos con nuestras metas, y a DIOS, quien ilumina nuestro andar y siempre camina a nuestro lado cubriéndonos con su manto divino.

1. RESUMEN EJECUTIVO

La institución educativa LEON XIII del municipio de Soacha está constituida por dos áreas fundamentales, en la primera denominada administrativa se encuentran las áreas de coordinaciones, secretarias, pagaduría y rectoría, la segunda denominada comunidad estudiantil está representada por 6600 estudiantes y 200 docentes, distribuidos en 3 sedes.

La institución no cuenta con un esquema de backup definido para realizar el respaldo de la información al área administrativa, donde a diario se realizan actualizaciones a la información de los estudiantes como pueden ser constancias, certificados, calificaciones.

En el área de las secretarias existe una rotación de personal muy continua, ya que la empresa contratista para suministrar el personal las rota por el resto de instituciones, esto ha permitido que las secretarias vengan con conocimientos de otras instituciones y así mismo se lleven los formatos o procedimientos de la institución, además por esta rotación, el compromiso de cada una por proteger la integridad de la información es muy poca permitiendo así que los datos sean borrados sin ningún reparo. Dentro de esta área existe una red LAN donde cada usuario tiene acceso a la información del otro usuario, lo que conlleva a producirse la perdida de confidencialidad al no tener restricciones de acceso; así mismo se

generan certificados o constancias sin el respectivo respaldo de quién fue la persona que lo realizo produciéndose el no repudio.

En el área de Coordinación y Secretaria sucede que a diario deben enviar reportes e informes a la Secretaria de Educación, estos envíos se realizan por medio del correo electrónico comercial (Hotmail), sin ningún tipo de seguridad, lo que pone en riesgo la integridad y confidencialidad de la información.

Para la información de los funcionarios, esta se encuentra en cada equipo de cómputo donde se tiene programado un .bat que realiza backup en otra partición del disco duro del mismo PC, también se realizan copias periódicas en un disco duro externo. En la actualidad no existe una persona que este monitoreando si se están realizando las copias correctamente, aun cuando la institución tiene una licencia del software Acronis para copias de seguridad, además las copias externas se realizan cuando la secretaria se acuerda de realizarlas, poniendo en un gran riesgo de pérdida la información académica de la institución, asimismo en cada equipo de cómputo no se ha realizado ningún tipo de hardening, lo que conlleva a pensar que es posible que se realice el backup, pero si el equipo se daña o es atacado la información estaría en riesgo.

OBJETIVO GENERAL: implementar un esquema de gestión de seguridad de la información en la Institución Educativa LEON XIII, donde se garanticen la triada CID, Confidencialidad, Integridad, Disponibilidad, además del no repudio, sobre los datos confidenciales de la institución.

OBJETIVOS ESPECIFICOS:

- Crear una política de seguridad de la información para la institución.
- Realizar un análisis de brechas para comprobar el estado actual y el desempeño real en materia de seguridad de la información.
- Efectuar un inventario de activos, clasificándolos por tipo de función como personas, servicios, información, hardware y software.
- Realizar un análisis de riesgos, para determinar las amenazas y vulnerabilidades de los activos de información.

- Establecer procedimientos donde quede plasmado la forma de realizar auditorías a la seguridad de la información, aplicar esteganografia y protección de los datos, esquemas de backup, hardening a nivel de sistema operativo y cifrado de la información para enviar por correo electrónico.

METODOLOGIA

Se creara un política de seguridad de la información donde serán consignados los lineamientos a seguir por el personal para el manejo de la información.

Por medio de la herramienta de Análisis de Brechas se realizara una investigación para comprobar el estado actual y el desempeño real en materia de seguridad de la información.

Se realizara un inventario a los activos ya que hacen referencia a todo lo que posee valor para la institución y por ende es necesario protegerlo, pueden ser clasificados por tipo de función como personas, servicios, información, hardware y software.

Los riesgos que se identifiquen estarán relacionados con las amenazas y vulnerabilidades de los activos de información, están clasificados como de tipo lógico, físico, locativo y legal.

Sera necesario realizar el diseño de las auditorías internas con el fin de verificar el correcto funcionamiento de las fases anteriores y aplicarlas con el fin de garantizar su efectividad.

Para generar un entorno seguro de la información que sea confidencial y exclusiva de la institución se asignara una ubicación en el equipo de la secretaria general ya que la oficina donde se encuentra el equipo siempre permanece bajo llave, allí en una partición se almacenara dicha información y se le aplicara la técnica de esteganografia y la clave se asignara a través del cifrado Vigenere para que permanezca segura y con la implementación del programa Veracrypt (Truecrypt) se ocultaran los datos, aplicando antes cifrado de Mason para la obtención de la clave.

En cada uno de los equipos de cómputo se establecerá un procedimiento de hardening para garantizar el mínimo de seguridad y que los datos de alguna forma estén seguros, dentro del esquema de backup incremental diario y full semanal.

Para el envío de información por correo electrónico y ya que la institución no cuenta con un correo corporativo, se implementara el cifrado simétrico, que con la utilización del programa AES Crypt, los datos enviados viajaran un poco más seguros garantizando su integridad y confidencialidad, además del no repudio ya que cada usuario deberá tener un correo electrónico.

RESULTADOS

Se tendrá un esquema de Gestión de Seguridad de la Información en la Institución Educativa LEON XIII, para lo cual se evidencian los siguientes resultados:

- Diseño de la Política de seguridad de la información.
- Informe del análisis de brechas el cual indicara el estado actual en temas de seguridad de la información.
- Clasificación del inventario de activos con la utilización de la metodología Magerit.
- Bajo el marco de trabajo NIST SP 800 se realiza el análisis de riesgos el cual contempla las siguientes etapas:
    - Identificación de amenazas
    - Identificación y valorización de vulnerabilidades
    - Identificación y valorización de impactos
    - Análisis y evaluación de riesgos
    - Definición del plan de tratamiento de riesgos
    - Implementación de controles
- Por último se realizan los diseños de las auditorías internas para determinar el nivel alcanzado en temas de seguridad de la información.
- Se construyen los procedimientos de protección de la información aplicando técnicas de Esteganografia, aplicación del software Veracrypt (Truecrypt) y esquema de Backup de la información, Hardening del sistema operativo y cifrado de la información con el software AES Crypt.

ALCANCE

El presente trabajo de grado incluye las fases de planeación y diseño, con los informes y procedimientos de cada fase para la gestión de la seguridad de la información. No incluye la implementación, pero queda la recomendación en la institución para que realicen la divulgación de todo lo consignado en este documento.

2. JUSTIFICACIÓN

Este proyecto pretende dar solución a la problemática presentada en la Institución Educativa LEON XIII en cuanto al respaldo y protección de la información en el área administrativa. Esta área es donde se maneja el activo más importante que es la información, y no cuenta con los controles necesarios que garanticen su seguridad. Los datos son consultados y actualizados por cualquier usuario con acceso al equipo de cómputo, donde pueden sustraer información y visualizar la del otro usuario, es importante enfatizar que la información es confidencial pero en la actualidad no se está protegiendo de la forma adecuada, esto llevaría a que los datos de los estudiantes o personal administrativo sea expuesto para fines fraudulentos.

La institución no cuenta con un correo corporativo, para el envío de información utilizan un correo comercial de Hotmail donde todas las secretarias tienen acceso, además la información enviada nunca va cifrada pudiendo caer en las manos equivocadas.

Debido a la rotación de personal, las secretarias no están concientizadas de la importancia en la seguridad de la información, no toman las medidas necesarias que ayuden a proteger los datos y permiten que otro usuario tenga acceso a la información de cada una, así como permitir el envío por correo de datos a nombre de ellas. Para lograr una mejor conceptualización de la problemática encontrada se realizó una encuesta para determinar el nivel de conocimientos en temas de seguridad de la información.

3. INDICADORES

Para lograr una efectividad, eficacia y eficiencia de la Gestión de Seguridad de la información en la Institución Educativa LEON XIII, se establecen cinco indicadores de gestión que permitirán realizar la medición al cumplimiento del esquema de gestión de seguridad, los tres primeros corresponden a las fases de planeación y diseño, el cuarto se tendrá en cuenta cuando la institución realice todo el despliegue del sistema:

- Backups realizados correctamente
- Activos inventariados
- Controles de riesgos
- Protección de la información
- Plan de concientización

Tabla 1. Indicador Backups realizados

INDICADOR – BACKUPS REALIZADOS CORRECTAMENTE					
DEFINICION					
El indicador permite verificar el porcentaje de backups realizados correctamente, se comprueba por el log del programa de backup.					
OBJETIVO					
Establecer la efectividad de los backups diarios de la información de la institución.					
DESCRIPCION DE VARIABLES		**FORMULA**		**FUENTE DE LA INFORMACION**	
ID1: Numero de backups realizados		(ID1 /ID2)*100		Logs del sistema de backups	
ID2: Numero de backups programados				Registro de backups por parte de tecnología	
METAS					
BAJA	60% - 75%	**MEDIA**	76 % - 90%	**ALTA**	91% - 100%
OBSERVACIONES					
Para la medición de este indicador es importante contar con los logs del sistema de backups					

Tabla 2. Activos inventariados

INDICADOR – ACTIVOS INVENTARIADOS
DEFINICION
El indicador permite verificar el porcentaje de activos que se han inventariado desde el inicio de la gestión de seguridad.
OBJETIVO
Identificar el total de activos que se han inventariado en la institución.

DESCRIPCION DE VARIABLES	FORMULA	FUENTE DE LA INFORMACION
ID5: Activos inventariados	(ID5 /ID6)*100	Formato de registro de inventario de activos
ID6: Total de activos de la institución		Área de tecnología

METAS					
BAJA	60% - 75%	**MEDIA**	76 % - 90%	**ALTA**	91% - 100%

OBSERVACIONES
Para la medición de este indicador es importante contar con los registros del inventario de activos

Tabla 3. Controles de riesgos

INDICADOR – CONTROLES DE RIESGOS					
DEFINICION					
El indicador permite verificar el porcentaje de controles de riesgos que se han identificado.					
OBJETIVO					
Establecer los controles de riesgos que se han identificado.					
DESCRIPCION DE VARIABLES		**FORMULA**		**FUENTE DE LA INFORMACION**	
ID7: Controles identificados		(ID7 /ID8)*100		Registro del tratamiento de riesgos	
ID8: Total de riesgos				Registro análisis de riesgos	
METAS					
BAJA	60% - 75%	**MEDIA**	76 % - 90%	**ALTA**	91% - 100%
OBSERVACIONES					
Para la medición de este indicador es importante contar con los registros del tratamiento de riesgos y análisis de riesgos					

Tabla 4. Protección de la información

INDICADOR – PROTECCION DE LA INFORMACION					
DEFINICION					
El indicador permite verificar la cantidad de información confidencial que se ha protegido.					
OBJETIVO					
Identificar la cantidad de información confidencial protegida					
DESCRIPCION DE VARIABLES		**FORMULA**		**FUENTE DE LA INFORMACION**	
ID9: Datos protegidos		(ID9 /ID10)*100		Registro de datos protegidos	
ID10: Total de datos				Registro activos identificados	
METAS					
BAJA	60% - 75%	**MEDIA**	76 % - 90%	**ALTA**	91% - 100%
OBSERVACIONES					
Para la medición de este indicador es importante contar con los registros de los datos protegidos y el registro de activos identificados					

Tabla 5. Plan de Concientización

<table>
<tr><th colspan="6">INDICADOR – PLAN DE CONCIENTIZACION</th></tr>
<tr><th colspan="6">DEFINICION</th></tr>
<tr><td colspan="6">El indicador permite verificar el porcentaje de toma de conciencia del personal referente a los temas de seguridad de la institución.</td></tr>
<tr><th colspan="6">OBJETIVO</th></tr>
<tr><td colspan="6">Establecer la efectividad de la generación de conciencia al personal en temas de seguridad de la información.</td></tr>
<tr><th colspan="2">DESCRIPCION DE VARIABLES</th><th colspan="2">FORMULA</th><th colspan="2">FUENTE DE LA INFORMACION</th></tr>
<tr><td colspan="2">ID11: Personal capacitado</td><td colspan="2" rowspan="2">(ID11 /ID12)*100</td><td colspan="2">Registro de capacitaciones</td></tr>
<tr><td colspan="2">ID12: Total del personal</td><td colspan="2">Secretaria general</td></tr>
<tr><th colspan="6">METAS</th></tr>
<tr><td>BAJA</td><td>60% - 75%</td><td>MEDIA</td><td>76 % - 90%</td><td>ALTA</td><td>91% - 100%</td></tr>
<tr><th colspan="6">OBSERVACIONES</th></tr>
<tr><td colspan="6">Para la medición de este indicador es importante contar con los registros de las capacitaciones y el dato de secretaria general sobre la nómina actual</td></tr>
</table>

4. SOLUCION

La solución a esta problemática viene dada por la construcción de un esquema de Gestión de Seguridad de la Información en la Institución Educativa LEON XIII, para lo cual contendrá los siguientes elementos:

- Política de seguridad de la información.
- Informe del análisis de brechas el cual indicara el estado actual en temas de seguridad de la información.
- Clasificación del inventario de activos con la utilización de la metodología Magerit.
- Informe del análisis de riesgos bajo el marco de trabajo NIST SP 800 el cual contiene las siguientes etapas:
    - Identificación de amenazas
    - Identificación y valorización de vulnerabilidades
    - Identificación y valorización de impactos
    - Análisis y evaluación de riesgos
    - Definición del plan de tratamiento de riesgos
    - Implementación de controles

- Diseño de las auditorías internas para determinar el nivel alcanzado en temas de seguridad de la información.
- Se establecen los procedimientos de protección de la información aplicando técnicas criptográficas como Vigenere y Esteganografia, ejecución del software Veracrypt (Truecrypt) con cifrado Mason y esquema de Backup de la información, Hardening del sistema operativo y cifrado de la información con el software AES Crypt.

Con esta solución se garantizara que el activo más importante de la Institución Educativa LEON XIII estará protegido ante ataques internos y externos, y los datos cumplirán con la triada CID de la seguridad de la información, Confidencialidad, Integridad y Disponibilidad, además del no repudio.

5. REFERENTES

La institución Educativa LEON XIII dentro de los proyectos de mejora tecnológica que cada año realiza, y dentro de la partida presupuestal que la alcaldía asigna, nunca ha determinado adecuar una solución al tema de la seguridad de la información, siendo este el activo más importante, siempre dan prioridad a los equipos de cómputo y mejoras locativas de las salas de informática.

6. MARCO TEÓRICO Y REFERENTES

Dentro del esquema de la Gestión de Seguridad de la Información en la Institución Educativa LEON XIII, se abordan conceptos como Triada CID, Política de seguridad de la información, análisis de brechas, inventario de activos, análisis de riesgos, Esteganografia, Vigenere, Vercrypt, Mason, Backup, Hardening y AES Crypt. A continuación se realiza una definición de cada uno:

- **Triada CID:** Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar su C-I-D:

    - Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
    - Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
    - Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. [1]
- **Política de seguridad de la información:** conjunto de normas y procedimientos establecidos por una organización para regular el uso de la información y de los sistemas que la tratan con el fin de mitigar el riesgo de pérdida, deterioro o acceso no autorizado a la misma. [2]
- **Análisis de brechas:** identificación de riesgos, definición de controles, identificación de requisitos legales, regulatorios, contractuales. [3]
- **Inventario de activos:** un activo de información es un elemento que posee información. Entre activos de información encontramos las bases de datos, acuerdos y/o contratos, documentos del sistema, ficheros, aplicaciones, software de información, equipos informáticos. [4]
- **Análisis de riesgos:** tiene como propósito determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo. [5]
- **Esteganografía:** La esteganografía es la disciplina en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros normalmente multimedia, llamados portadores, de modo que no se perciba su existencia. Es una mezcla de artes y técnicas que se combinan para conformar la práctica de ocultar y enviar información sensible en un portador que pueda pasar desapercibido. [6]
- **Vigenere:** El cifrado Vigenère es un criptosistema simétrico, es decir, utiliza la misma clave para cifrar y descifrar. El cifrado Vigenère se asemeja mucho al cifrado César, pero su diferencia radica en que el primero utiliza una clave más larga para contrarrestar el gran problema del cifrado César: el hecho de

que una letra sólo puede ser codificada de una forma. Para resolver este problema, se utiliza una palabra clave en lugar de un carácter simple. [7]

- **Veracrypt (Truecrypt):** Vercrypt, al igual que Truecrypt, cuando crea un nuevo Contenedor o Volumen, te da lo posibilidad de crear un Hidden Veracrypt (Truecrypt) Volume, o lo que es lo mismo: Un volumen oculto. ¿Para qué sirve este volumen y cómo funciona? Fácil, el volumen o contenedor oculto sirve para tener los datos a salvo incluso cuando una persona se ve forzado a decir su contraseña. De tal manera que Veracrypt (Truecrypt) almacenará dos contraseñas distintas para dos volúmenes distintos. De esta forma si introducimos una contraseña se mostrará un contenido, y si introducimos otra contraseña se mostrará un contenido distinto. [8]
- **Mason:** El cifrado francmasón es un cifrado por sustitución simple que cambia las letras por símbolos. Sin embargo, el uso de símbolos no impide el criptoanálisis, y el criptoanálisis es idéntico al de otros métodos de cifrado por substitución simple.

  Llamado también “cifra Pigpen” este método de cifrado fue utilizado por los masones en el siglo XVIII para preservar la privacidad de sus archivos. [9]
- **Backup:** el backup o copia de seguridad, es la copia total o parcial de información importante como respaldo frente a eventualidades. La copia de seguridad debería ser guardada en un soporte almacenamiento diferente del original, para evitar que un fallo en el mismo pueda estropear el original y la copia. [10]
- **Acronis:** Acronis True Image es una aplicación para la creación de imágenes de disco, especial para crear sistemas de respaldos y recuperación de PCs. Es desarrollada por la empresa Acronis.

  Es una aplicación muy sencilla de usar, gracias a su interfaz que posee un claro asistente.

  Fue lanzado en 2002 y podía crear una imagen de la unidad que estaba siendo ejecutada sin tener que pasar al modo DOS. Las últimas versiones también permiten crear respaldos online de los datos.

Soporta múltiples sistemas de archivos como ser NTFS, FAT16, FAT32, ext2, ext3, ReiserFS, Reiser4, Linux Swap; además también puede copiar cualquier otro sistema de archivos en modo raw, capturando una imagen de todos los sectores de un disco. Este modo también sirve para sistemas de archivos que se han corrompido. [11]

- **Hardening:** es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc. Innecesarios en el sistema así como cerrando puertos que tampoco estén en uso además de muchas otros métodos y técnicas. [12] [13]
- **AES Crypt:** es un software de cifrado de archivos disponibles en varios sistemas operativos que utiliza el estándar de la industria estándar de cifrado avanzado (AES) para cifrar archivos de forma fácil y segura. [14]

La Institución Educativa LEON XIII, al ser una entidad pública, genera una gran cantidad de rotación de personal al momento de suceder el cambio de gobierno municipal, ha sido para conocimiento público que en cada gobierno se generan proyectos costosos que buscan solucionar las diferentes problemáticas encontradas en cada una de las instituciones educativas, se han construido instituciones modernas, se han implementado servicios de internet cubriendo la totalidad de instituciones, se han realizado contratos para suministrar equipos de cómputo a las salas de informática, se han realizado convenios con Computadores para Educar con el fin de implementar las aulas TIC y se ha realizado inversión en la creación de redes LAN para el intercambio de información al interior de cada institución, lo que nunca han hecho o han realizado, es una inversión considerable en los temas de protección del activo más importante en una organización y es la información. Cada institución se encarga de estructurar todos los datos que a diario manipulan, tanto en archivo físico como digital, pero ninguna se preocupa por mantener backups de la información en sitios externos a la institución, tampoco toman la precaución de proteger los datos que circulan por la red, estos se envían de forma tranquila y sin seguridad, además cada uno de los funcionarios no tienen la conciencia de la importancia de proteger este bien, así como los equipos para su operación.

7. METODOLOGÍA

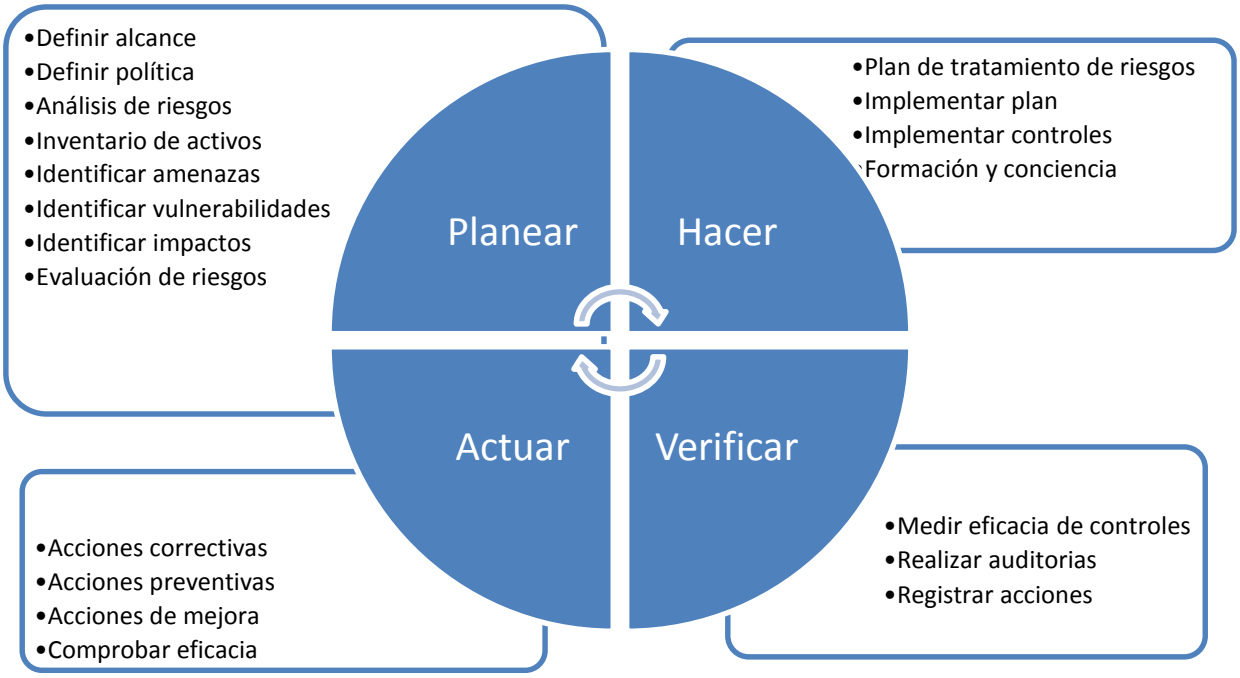
Inicialmente se realizó un levantamiento de información en la Institución Educativa LEON XIII, bajo el esquema propuesto por la norma ISO 27001, donde el sistema de gestión se basa en el ciclo PHVA (Planear, Hacer, Verificar y Actuar).

Dentro de la etapa de **Planificación** se realiza toda la gestión de creación de política, definición del alcance, análisis de riesgos para determinar cómo se encuentra la institución en la actualidad, luego de este análisis se determina cuál será su tratamiento y así implementar los respectivos controles de seguridad.

En la etapa **Hacer** se realiza la implementación del plan de tratamiento de riesgos, así como el proceso de formación en temas de seguridad para todo el personal y su respectiva toma de conciencia, además se realiza la definición de los métodos de medición que permitan evaluar la eficacia de estos controles.
La fase de **Verificación** comprueba que todo lo que se ha implementado esté funcionando de manera correcta, la forma más adecuada de realizar esta comprobación es por medio de una auditoria interna.

Con la etapa **Actuar** se realiza la implementación de acciones correctivas, preventivas y de mejora, las cuales son resultantes de las auditorias y surgen con el fin de lograr una gestión eficiente.

Figura 1. Ciclo PHVA



7.1 Encuesta

Con el fin de determinar el grado de conocimientos del personal en los temas referentes a la seguridad de los datos, se utilizó el instrumento de medición dentro del **Procedimiento Encuesta**. (Ver Anexo 1)

7.2 Política de Seguridad de la Información

Se diseñó la **Política de seguridad de la información**, donde se estableció de forma general los aspectos a tener en cuenta para el manejo de la información, donde se incluye: contexto general, objetivos, alcance, responsabilidades, tiempos de revisión, mecanismos de difusión y consecuencias. (Ver Anexo 2)

7.3 Análisis de Brechas

Por medio de la herramienta de Análisis de Brechas se realizó una investigación para comprobar el estado actual y el desempeño real en materia de seguridad de la Institución Educativa LEON XIII, allí se determinaran los cuatro pasos generales de esta herramienta que consisten en:

- Decidir cuál es la situación actual que se desea analizar y se quiere resolver.
- Delinear el objetivo o estado futuro deseado.
- Identificar la brecha entre el estado actual y el objetivo.
- Determinar los planes y las acciones requeridas para alcanzar el estado deseado. [15]

Dentro de esta fase es necesario diligenciar el formato dentro del **Procedimiento Análisis de Brechas** con los resultados arrojados en cada uno de los pasos anteriores a través de la investigación realizada. (Ver Anexo 3)

7.4 Inventario y Clasificación de Activos de Información

Los activos hacen referencia a toda la información que posee valor para la empresa y por ende es necesario protegerla, pueden ser clasificadas por tipo de función como personas, servicios, información, hardware y software.

Dentro de las personas que por su conocimiento, experiencia y habilidades dentro del proceso se identifican:

- Los usuarios del sistema
- Personal de la institución
- Personal temporal
- Contratistas

Los servicios pueden ser tanto internos como externos:

- Gestión administrativa
- Correo electrónico
- Acceso a internet
- Acceso a la red

La información dentro de su forma física como digital se encuentra:

- Archivos de datos
- Bases de datos
- Contratos
- Documentos de recursos humanos, docentes
- Documentos tecnología
- Documentos de proveedores
- Documentos de estudiantes
- Documentación del sistema

El hardware crítico utilizado en cada uno de los procesos como:

- Equipos de cómputo
- Equipos de comunicaciones
- Dispositivos de seguridad
- Unidades de backup
- Unidades de almacenamiento

El software está comprendido por:

- Herramientas de ofimática
- Gestores de bases de datos
- Aplicaciones específicas de la institución

Para cada uno de los activos identificados se debe especificar a qué tipo de dato personal pertenece, puede ser:

- Dato público: datos contenidos en documentos públicos
- Dato semiprivado: aquel dato que puede ser de interés general
- Dato privado: únicamente con acceso al titular de la información

El documento que se generara en esta fase se denomina **Formato Inventario y Clasificación de Activos de Información** y deberá tener contemplada la triada de Confidencialidad, Integridad y Disponibilidad junto con la valoración de cada activo de información de la siguiente forma:

Tabla 6. Impacto perdida de confidencialidad

TIPO DE FUNCION	CONFIDENCIALIDAD
Personas	Uso inadecuado de la información propia del cargo
Servicios	Uso no autorizado del activo
Información	Acceso no autorizado al activo por personal no autorizado
Hardware	Acceso a la configuración del activo sin autorización
Software	Conocimiento de la parametrización del activo

Tabla 7. Valoración Confidencialidad

CRITERIO	DESCRIPCION	EXPLICACION
A	**Alto**	El acceso no autorizado o divulgación de la información gestionada por este activo impacta de forma negativa la institución.
M	**Medio**	El acceso no autorizado o divulgación de la información gestionada por este activo impacta de forma negativa no solo el proceso evaluado sino otros procesos de la institución.
B	**Bajo**	El acceso no autorizado o divulgación de la información gestionada por este activo impacta levemente de forma negativa la institución.
MB	**Muy bajo**	El acceso no autorizado o divulgación de la información gestionada por este activo NO impacta de forma negativa la institución.

Tabla 8. Impacto perdida de Integridad

TIPO DE FUNCION	INTEGRIDAD
Personas	Generación de datos incorrectos
Servicios	Se valora la exactitud en la prestación del servicio
Información	Errores en el procesamiento del sistema
Hardware	Configuración alterada indebidamente
Software	Modificación en la parametrización del software

Tabla 9. Valoración Integridad

CRITERIO	DESCRIPCION	EXPLICACION
A	**Alto**	La pérdida del estado completo del activo impacta de forma negativa la institución.

M	**Medio**	La pérdida del estado completo del activo impacta de forma negativa no solo el proceso evaluado sino otros procesos de la institución.
B	**Bajo**	La pérdida del estado completo del activo impacta levemente de forma negativa la institución.
MB	**Muy bajo**	La pérdida del estado completo del activo NO impacta de forma negativa la institución.

Tabla 10. Impacto perdida Disponibilidad

TIPO DE FUNCION	DISPONIBILIDAD
Personas	En el proceso no se encuentra disponible la persona
Servicios	No se puede tener acceso al activo o no está disponible
Información	No se puede acceder o utilizar el activo de información
Hardware	No se puede acceder o utilizar el activo
Software	No se puede acceder o utilizar el activo

Tabla 11. Valoración Disponibilidad

CRITERIO	DESCRIPCION	EXPLICACION
A	**Alto**	La no disponibilidad o ausencia del activo impacta de forma negativa la institución.
M	**Medio**	La no disponibilidad o ausencia del activo impacta de forma negativa no solo el proceso evaluado sino otros procesos de la institución.
B	**Bajo**	La no disponibilidad o ausencia del activo impacta levemente de forma negativa la institución.
MB	**Muy bajo**	La no disponibilidad o ausencia del activo NO impacta de forma negativa la institución.

Siguiendo la metodología Magerit los activos de información se pueden clasificar en los siguientes tipos:

- Servicios: son los procesos de negocio de la organización.
- Datos e información: todo lo que se procesa internamente.
- Aplicaciones de software.
- Equipos de cómputo.
- Personal: todas las personas con vínculo laboral.

- Redes de comunicaciones: todo lo que permite la interconexión de la compañía.
- Soportes de información: dispositivos físicos de almacenamiento.
- Equipos auxiliares: dispositivos externos diferentes a los de cómputo que ayudan en las tareas.
- Instalaciones: infraestructura que soporta la organización.

Magerit es una metodología práctica para gestionar riesgos elaborada por el Consejo Superior de Administración Electrónica de España, ofrece un método sistemático para análisis de riesgos e implementar medidas de control más adecuadas, dentro de sus característica principales se encuentran:

- Analiza el impacto que genera la violación de seguridad
- Presenta una guía completa paso a paso para analizar riesgos
- Esta metodología se divide en tres libros
- El primer libro es el Método, referente a la estructura del modelo de gestión de riesgos
- El segundo libro es Catalogo de elementos con un inventario de los activos principales
- El tercer libro Guía de técnicas, están las técnicas para análisis de riesgos, tablas de ejemplos, algoritmos, arboles de ataque
- Está alineado con los estándares ISO
- Metodología enfocada a empresas que hasta ahora inician con la Gestión de Seguridad de la Información

Esta metodología es la que mejor se adapta a la Institución Educativa LEON XIII, ya que su esencia se enfoca en las empresas que están iniciando con la Gestión de Seguridad de la Información, además enfoca los esfuerzos en los riesgos que pueden ser más críticos para la organización. Esta metodología se convierte en el punto de partida para obtener la certificación en la norma ISO 27000 ya que su estructura está alineada con los estándares de la norma ISO. (Ver Anexo 4)

La metodología principal sobre la que se basa este proyecto es el SGSI Sistema de Gestión de Seguridad de la Información que se basa en la norma ISO 27001, con ella se pretende reducir los riesgos de la organización en temas de información.
Para la gestión de riesgos se debe basar en la metodología NISP SP 800 que documenta la forma correcta de realizar un análisis de riesgos y la ejecución de las acciones que conlleven a lograr el nivel de seguridad deseado.

7.5 Análisis de Riesgos

7.5.1 Identificación de amenazas

Con el inventario de activos de información realizado se procede a identificar las amenazas que pueden tener un gran impacto en la información y a la vez pueden afectar a uno o varios activos. Las amenazas se pueden clasificar como origen natural, errores y fallos no intencionados, ataques intencionados.
Las amenazas de origen natural se pueden identificar en la siguiente tabla:

Tabla 12. Amenazas de origen natural

AMENAZA	DESCRIPCION
Fuego	Un incendio acabaría con todos los recursos
Daños por agua	Una inundación acabaría con todos los recursos
Desastres naturales	Incidentes naturales que ocurren sin intervención humana

Las amenazas de errores y fallos no intencionados se relacionan en la tabla siguiente:

Tabla 13. Amenazas de errores y fallos no intencionados

AMENAZA	DESCRIPCION
Errores de usuarios	Fallas provocadas por los usuarios
Errores de Administrador	Fallas a causa de personal con privilegios administrativos
Errores de configuración	Configuraciones con datos equivocados
Software dañino	Propagación de virus, troyanos
Alteración de la información	Variación accidental de los datos

Destrucción de información	Perdida accidental de los datos
Vulnerabilidades del software	Fallas en el código que permiten alteraciones al software
Errores de mantenimiento en software	Fallas en las actualizaciones de software
Errores de mantenimiento en hardware	Fallas en las actualizaciones de hardware
Indisponibilidad del personal	Ausencia no prevista por el personal

Las amenazas de ataques intencionados están relacionados en la siguiente tabla:

Tabla 14. Amenazas de ataques intencionados

AMENAZA	DESCRIPCION
Manipulación de configuración	Cambios no autorizados en las configuraciones de equipos o software
Suplantación de identidad	Utilización indebida de los privilegios de un usuario
Abuso de privilegios	Utilizar los permisos concedidos para otros fines
Difusión de software dañino	Propagación intencionada de virus, troyanos
Acceso no autorizado	Ingreso al sistema aprovechando un fallo del mismo
Análisis de trafico	Analizar el contenido de las comunicaciones origen – destino
Repudio	Negación de actividades realizadas
Modificación de la información	Alteración intencional de los datos
Destrucción de la información	Eliminación intencional de los datos
Denegación de servicio	Provocar la caída del sistema por insuficiencia de los recursos
Indisponibilidad del personal	Ausencia provocada del puesto de trabajo

Esta información será diligenciada en la sección **"Identificación de Amenazas"**, consta de las amenazas identificadas en la institución y serán consignadas en su totalidad.

7.5.2 Identificación y valorización de vulnerabilidades

La vulnerabilidad está definida como una debilidad o incapacidad de resistir una amenaza que al ser explotada afectaría los activos de la organización.
Estas vulnerabilidades luego de ser identificadas deben valorarse y priorizarse, relacionándolas al detalle con el fin de observar la frecuencia de ocurrencia y así poder evaluarlas de acuerdo a la siguiente tabla:

Tabla 15. Valoración de Vulnerabilidades

VALOR	PERIODICIDAD	PROBABILIDAD DE OCURRENCIA
Muy Frecuente (MF)	A diario	75% – 100%
Frecuente (F)	Una vez al mes	50% - 75%
Frecuencia Normal (FN)	Una vez al año	25% - 50%
Poco Frecuente (PF)	Cada varios años	0 – 25%

Esta información deberá registrarse en la sección **"Identificación de Vulnerabilidades"**:

7.5.3 Identificación y valorización de impactos

El impacto es el daño causado en el activo por la materialización de una amenaza, y se evalúan de acuerdo al tipo de perdida que se presente, pueden ser de tipo organizacional o de tipo técnico.
Las pérdidas de tipo organizacional se clasifican económicas y en imagen, las económicas tienen una valoración como se muestra en la siguiente tabla:

Tabla 16. Perdidas económicas

ESCALA DE VALORACION	ESCALA CUANTITATIVA	DESCRIPCION
Muy Bajo (MB)	1	Costos entre 10.000 y 100.000
Bajo (B)	2	Costos entre 100.001 y 1.000.000

Medio (M)	3	Costos entre 1.000.001 y 5.000.000
Alto (A)	4	Costos entre 5.000.001 y 10.000.000
Muy Alto (MA)	5	Costos mayores a 10.000.000

Las pérdidas de imagen se visualizan en la siguiente tabla:

Tabla 17. Perdidas de imagen

ESCALA DE VALORACION	ESCALA CUANTITATIVA	DESCRIPCION
Muy Bajo (MB)	1	Perdida leve de la imagen
Bajo (B)	2	Perdida moderada
Medio (M)	3	Pérdida importante
Alto (A)	4	Perdida alta
Muy Alto (MA)	5	Perdida muy alta

Las pérdidas de tipo técnico se clasifican en Confidencialidad, Integridad y disponibilidad; las pérdidas de confidencialidad tienen una valoración como se muestra en la siguiente tabla:

Tabla 18. Pérdidas de Confidencialidad

ESCALA DE VALORACION	ESCALA CUANTITATIVA	DESCRIPCION
Muy Bajo (MB)	1	Mínimos datos expuestos y no sensibles
Bajo (B)	2	Mínimos datos expuestos
Medio (M)	3	Importante cantidad de datos no sensibles expuestos
Alto (A)	4	Importante cantidad de datos expuestos
Muy Alto (MA)	5	Totalidad de los datos expuestos

Las pérdidas de Integridad se valorizan en la siguiente tabla:

Tabla 19. Pérdidas de Integridad

ESCALA DE VALORACION	ESCALA CUANTITATIVA	DESCRIPCION
Muy Bajo (MB)	1	Mínimos datos dañados
Bajo (B)	2	Mínimos datos importantes dañados

Medio (M)	3	Gran cantidad de datos dañados
Alto (A)	4	Gran cantidad de datos importantes dañados
Muy Alto (MA)	5	Totalidad de los datos dañados

Las pérdidas de disponibilidad están valorizadas en la tabla siguiente:

Tabla 20. Pérdidas de Disponibilidad

ESCALA DE VALORACION	ESCALA CUANTITATIVA	DESCRIPCION
Muy Bajo (MB)	1	Interrupción mínima del servicio
Bajo (B)	2	Interrupción mínima de los servicios básicos
Medio (M)	3	Interrupción amplia de los servicios
Alto (A)	4	Interrupción amplia de los servicios básicos
Muy Alto (MA)	5	Interrupción total de los datos servicios

Esta información será consignada en la sección **"Identificación y Valorización de Impactos"** además se obtendrán los promedios de valoración y se calificara el posible daño de acuerdo a la siguiente tabla:

Tabla 21. Escala de valoración del Impacto

ESCALA DE VALORACION	ESCALA CUANTITATIVA	DESCRIPCION
Muy Bajo (MB)	1	Daño insignificante
Bajo (B)	2	Daño menor
Medio (M)	3	Daño importante
Alto (A)	4	Daño grave
Muy Alto (MA)	5	Daño muy grave

7.5.4 Análisis y evaluación de riesgos

Los riesgos que se identifiquen estarán relacionados con las amenazas y vulnerabilidades de los activos de información, están clasificados como de tipo lógico, físico, locativo y legal.

Dentro del tipo lógico se encuentran:

- Control de acceso

- Manejo de la información
- Manejo del software
- Entrada y salida de los datos

Para el tipo físico se determinan:

- Utilización de los equipos
- Cuidado de los equipos

En el tipo locativo se tienen en cuenta:

- Ubicación de los equipos dentro de la organización

Para el tipo legal se verifica:

- Cumplimiento legal

La valoración de los riesgos encontrados está dado por el valor de la vulnerabilidad (Muy Frecuente (MF), Frecuente (F), Frecuencia Normal (FN), Poco Frecuente (PF)) y su impacto (Muy Bajo (MB), Bajo (B), Medio (M), Alto (A), Muy Alto (MA)) sobre el activo de información, este cruce de valores se puede observar en la siguiente matriz cualitativa:

Tabla 22. Matriz cualitativa de riesgos

RIESGO		**VULNERABILIDAD**			
		PF(1)	FN(2)	F(3)	MF(4)
IMPACTO	MA(5)	A(5)	MA(10)	MA(15)	MA(20)
	A(4)	M(4)	A(8)	MA(12)	MA(16)
	M(3)	B(3)	M(6)	A(9)	MA(12)
	B(2)	MB(2)	B(4)	M(6)	A(8)
	MB(1)	MB(1)	MB(2)	B(3)	M(4)

La matriz cuantitativa que determina el valor final del riesgo se observa en la siguiente imagen:

Tabla 23. Matriz cuantitativa de riesgos

CLASE	VALORACION CUALITATIVA	VALORACION CUANTITATIVA
CRITICO	Muy Alto	10 a 20
GRAVE	Alto	5 a 9
MODERADO	Medio	1 a 4

Los datos anteriores junto con la calificación de cada riesgo se registran en la sección denominada **"Análisis y Evaluación de Riesgos"**.

7.5.5 Definición del plan de tratamiento de riesgos

El plan determinado para el tratamiento de riesgos contempla las medidas que se tomaran las cuales serán evaluadas y tendrán un seguimiento constante, donde se actualice la valorización de las vulnerabilidades, el impacto y los riesgos.

Las siguientes son las medidas a tener en cuenta en cada riesgo identificado:

Tabla 24. Tratamiento de Riesgos

MEDIDA	DESCRIPCION
Evitar el riesgo	Se utiliza cuando se aplican mejoras en el proceso para evitar el riesgo
Reducir el riesgo	Se logra optimizando los procedimientos
Dispersar el riesgo	Para implementar esta medida se distribuye el riesgo en varios lugares
Transferir el riesgo	Se identifica en pasar el riesgo de un lugar a otro o entre procesos
Asumir el riesgo	Cuando el riesgo es asumido es necesario identificar el responsable que realizara la mitigación

Es necesario determinar los responsables y fechas de implementación.

7.5.6 Implementación de controles

Luego de tener el documento de tratamiento de riesgos actualizado donde se detallan las exposiciones del sistema y la priorización a solucionar, se define el plazo para contrarrestar las amenazas y vulnerabilidades, ya sea a corto, mediano y largo plazo.

En el corto plazo serán atacados los activos que posean el nivel de riesgo más alto, seguido de los riesgos de nivel medio que aunque son relevantes pueden ser atacados a mediano plazo, finalmente los activos con un nivel de riesgo bajo pueden ser aceptados cuando el control representa un mayor costo que el costo representado por la pérdida producida por el evento.

Existen algunos factores de vital importancia a la hora de implementar los controles y que deben tenerse en cuenta, como son:

- La efectividad de las opciones recomendadas
- La adecuación a leyes y normas existentes
- El impacto operacional de las modificaciones
- La confiabilidad de tales controles

El control implementado tiende a reducir el impacto que produce una amenaza o la frecuencia con la que ocurre, y el objetivo principal es reducir el nivel de riesgo a un nivel aceptable que no afecte la organización. (Ver Anexo 5)

7.6 Auditoria

Sera necesario realizar auditorías internas con el fin de verificar el correcto funcionamiento de las fases anteriores y de ser posible volver a evaluarlas para garantizar su efectividad. Esta revisión deberá hacerse trimestralmente y estará basada en el documento “**Procedimiento Auditorías Internas”.**

Luego de realizar las auditorías a cada una de las fases utilizando el formato de resultados y teniendo el plan de acción a ejecutar, se procede a realizar el plan de acciones correctivas y preventivas, cada una de estas acciones tendrá un formato para ser diligenciado:

Tabla 25. Planes de mejora

PLAN DE MEJORA			LÍDER DE LA FASE:		
ANÁLISIS DE CAUSAS					
FASE	**CAUSA**	**SUBCAUSA**	**FUENTE**	**CORRECCION PROPUESTA**	
ACCIONES A IMPLEMENTAR					
DE MEJORA	**PREVENTIVA**	**CORRECTIVA**	**RESPONSABLE**	**FECHA INICIO**	**FECHA FIN**
FECHA DE SEGUIMIENTO:			**RESPONSABLE:**		

El formato de las auditorías internas se encuentra como anexo. (Ver Anexo 6)

7.7 Procedimientos protección información

Se establecen los procedimientos de protección de la información con el fin de brindar un mejor aseguramiento:

- Aplicar técnicas de criptografía Vigenere y Esteganografia (Ver Anexo 7)
- Cifrado Mason y ejecución del software Veracrypt (Truecrypt) para protección de los datos (Ver Anexo 8)
- Determinar esquema de Backup de la información (Ver Anexo 9)
- Aplicar Hardening del sistema operativo (Ver Anexo 10)
- Cifrado de la información con el software AES Crypt. (Ver Anexo 11)

7. RESULTADOS Y DISCUSIÓN

Con la Gestión de Seguridad en la Institución Educativa LEON XIII, se logra tener un mayor control en temas de seguridad, ya que los documentos confidenciales van a estar protegidos, así como la información que viaja a través de la red; todo esto se logra con la rigurosa aplicación de cada uno de los siguientes elementos:

- Aplicación de los componentes de la política de seguridad de la información tanto del personal interno, como contratistas y proveedores de la institución.
- Contención de las brechas y problemas de seguridad de la información encontrados durante el análisis realizado.
- Mantener actualizado el inventario de activos, revisando su adecuada clasificación y mitigan al máximo las amenazas que se encuentren, así como la aplicación de remediación de riesgos.

Para todos los procesos internos aplicar los procedimientos establecidos en temas de seguridad como son:

- Auditorías a la seguridad de la información
- Esteganografia y protección de los datos
- Esquemas de backup
- Hardening a nivel de sistema operativo
- Cifrado de la información para enviar por correo electrónico

Cada uno de estos procedimientos se encuentran como anexos, así como los siguientes documentos:

- Encuesta
- Política de seguridad de la información
- Análisis de brechas
- Inventario y clasificación de activos de información
- Análisis de riesgos
- Informe ejecutivo

La construcción de estos anexos se realizó con toda la información suministrada por la Institución Educativa LEON XIII, y basados en los conocimientos adquiridos en la Especialización que con cada herramienta e información aportada fue crucial para lograr un esquema de Gestión de Seguridad acorde a las necesidades de la institución que primordialmente eran las falencias en la triada CID, Confidencialidad, Integridad, Disponibilidad, además del no repudio, sobre los datos confidenciales de la institución.

8. CONCLUSIONES

Con la aplicación de cada uno de estos procedimientos y actualización de los formatos diseñados, se lograra una Gestión más eficiente en temas de seguridad de la información, y lo más importante, se logra brindar una protección más acertada a los datos de la institución.

La Institución Educativa LEON XIII en su afán de proteger la información ha adaptado de una forma muy acertada cada uno de los procedimientos aquí descritos, garantizando que cada uno de sus datos adopten la triada CID de acuerdo a la necesidad, además de garantizar el no repudio en los procesos internos de envío de información.

Durante el proceso la construcción de los anexos se pudo evidenciar que la institución no tenía adoptado el término de seguridad de la información, ya que tanto usuarios como archivos actuaban de manera inconsciente y no determinaban las consecuencias de operar de forma insegura, teniendo en cuenta que allí reposan todos los archivos físicos y magnéticos de los estudiantes desde su fecha de fundación en el año 1978.

Durante este proceso se adquirieron conocimientos en temas referentes a los procesos educativos de forma administrativa que se manejan al interior de la institución.

Como recomendación principal se sugiere a la institución darle continuidad a la gestión de seguridad en el presente modelo para que pueda ser revisado periódicamente garantizando el cumplimiento de los objetivos de la institución, para esto es muy importante la revisión de los indicadores que permitan realizar la medición del modelo, que estará soportado por los registros que se establezcan.

Es muy importante que la dirección en cabeza del señor rector esté al tanto de todo lo que ocurre con la Gestión de Seguridad, para ello se deberán seguir las siguientes recomendaciones:

- Generar un informe con las incidencias encontradas durante las auditorías internas
- Las reuniones del comité de Gestión de Seguridad deben generar informes con el estado actual del sistema
- Reportar el total de incidencias encontradas y la solución a las mismas
- Revisar el cumplimiento de los objetivos establecidos en cada fase

Después que la dirección revise estos documentos se debe establecer:

- Costos que impliquen las mejoras al sistema
- Volver a realizar el análisis de riesgos y su plan de tratamiento en caso que ocurran cambios importantes
- Revisar y actualizar los procedimientos establecidos

Se recomienda realizar una auditoria anual a todo el modelo de Gestión de Seguridad teniendo en cuenta todos los riesgos, amenazas y vulnerabilidades encontradas. Esta auditoria debe ser realizada por personal interno de la organización pero que no haya participado en la implementación de la Seguridad de la Información. Se pueden programar varias auditorías al año enfocándose en las fases donde se observe una mayor debilidad.

Para obtener una mejor visión de la Gestión de Seguridad y teniendo en cuenta los indicadores encargados de realizar la medición del sistema, se propone la creación de un cuadro de mandos donde se puedan administrar estos indicadores.

9. BIBLIOGRAFÍA

[1] iso27000.es, «http://www.iso27000.es,» 2012. [En línea]. Available: http://www.iso27000.es/sgsi.html. [Último acceso: 24 04 2016].

[2] I. Forum, «http://www.protegetuinformacion.com/,» [En línea]. Available: http://www.protegetuinformacion.com/perfil_tema.php?id_perfil=6&id_tema=56. [Último acceso: 24 04 2016].

[3] S. I. Colombia, «http://seguridadinformacioncolombia.blogspot.com.co/,» [En línea]. Available: http://seguridadinformacioncolombia.blogspot.com.co/2010/06/declaracion-de-aplicabilidad-statement.html. [Último acceso: 24 04 2016].

[4] PMG-SSI, «http://www.pmg-ssi.com/,» [En línea]. Available: http://www.pmg-ssi.com/2014/03/iso-27001-y-el-inventario-de-activos-de-la-informacion/. [Último acceso: 24 04 2016].

[5] M. Erb, «https://protejete.wordpress.com,» [En línea]. Available: https://protejete.wordpress.com/gdr_principal/analisis_riesgo/. [Último acceso: 24 04 2016].

[6] Gits Informatica, «http://www.gitsinformatica.com/,» [En línea]. Available: http://www.gitsinformatica.com/criptografia.html. [Último acceso: 24 04 2016].

[7] es.ccm.net, «http://es.ccm.net,» [En línea]. Available: http://es.ccm.net/contents/143-el-cifrado-vigenere. [Último acceso: 24 04 2016].

[8] veracrypt.codeplex, «https://veracrypt.codeplex.com/,» [En línea]. Available: https://veracrypt.codeplex.com/. [Último acceso: 24 04 2016].

[9] jc-mouse.net, «http://www.jc-mouse.net,» [En línea]. Available: http://www.jc-mouse.net/java/cifrado-francmason-pigpen. [Último acceso: 24 04 2016].

[10] Alegsa, «http://www.alegsa.com.ar,» [En línea]. Available: http://www.alegsa.com.ar/Dic/backup.php. [Último acceso: 24 04 2016].

[11] alegsa.com.ar, «http://www.alegsa.com.ar,» [En línea]. Available: http://www.alegsa.com.ar/Dic/acronis%20true%20image.php. [Último acceso: 24 04 2016].

[12] Smartekh, «http://blog.smartekh.com,» [En línea]. Available: http://blog.smartekh.com/%C2%BFque-es-hardening/. [Último acceso: 24 04 2016].

[13] hardenwindows7forsecurity, «http://hardenwindows7forsecurity.com/,» [En línea]. Available: http://hardenwindows7forsecurity.com/. [Último acceso: 24 04 2016].

[14] Packetizer, Inc., «https://www.aescrypt.com/,» [En línea]. Available: https://www.aescrypt.com/. [Último acceso: 24 04 2016].

[15] R. Kelly, «robdkelly.com,» 2009. [En línea]. Available: http://robdkelly.com/blog/getting-things-done/gap-analisys/. [Último acceso: 15 09 2015].

10. ANEXOS

Anexo 1. Procedimiento encuesta

Anexo 2. Política de seguridad de la información

Anexo 3. Procedimiento análisis de brechas

Anexo 4. Formato inventario y clasificación de activos de información

Anexo 5. Formato análisis de riesgos

Anexo 6. Procedimiento auditorías internas

Anexo 7. Procedimiento Esteganografia

Anexo 8. Procedimiento Veracript

Anexo 9. Procedimiento esquema de backup

Anexo 10. Procedimiento Hardening SO

Anexo 11. Procedimiento AES Crypt