	UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA			
	Documento	Código	Fecha	Revisión
FORMATO HOJA DE RESUMEN PARA TRABAJO DE GRADO	F-AC-DBL-007	10-04-2012	A	
Dependencia	Aprobado		Pág.	
DIVISIÓN DE BIBLIOTECA	SUBDIRECTOR ACADEMICO		1(122)	

RESUMEN – TRABAJO DE GRADO

AUTORES	LEIDY YOANA BAYONA MORENO, KATHERINE MEJIA TAMARA, BEATRIZ EUGENIA SARMIENTO CARVAJALINO		
FACULTAD	FACULTAD DE INGENIERIAS		
PLAN DE ESTUDIOS	ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS		
DIRECTOR	TORCOROMA VELASQUEZ PEREZ		
TÍTULO DE LA TESIS	CREACIÓN DE UN MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA DEPENDENCIA SECRETARIA DE LA INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELEN DE CÚCUTA		
RESUMEN (70 palabras aproximadamente)			
<p>La creación de un manual de políticas de seguridad de la información para la dependencia secretaria de la Institución Educativa Nuestra Señora de Belén de Cúcuta, desarrollado mediante análisis de los procesos que se realizan; con el fin de minimizar los riesgos a los que están expuestos con respecto a la información, que permitirá la construcción del documento final para establecer las medidas o protocolos de seguridad de la información, en forma organizada, para establecer la integridad, confidencialidad y disponibilidad de la información del centro educativo.</p>			
CARACTERÍSTICAS			
PÁGINAS: 122	PLANOS: 0	ILUSTRACIONES: 12	CD-ROM: 1



CREACIÓN DE UN MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
PARA LA DEPENDENCIA SECRETARIA DE LA INSTITUCIÓN EDUCATIVA NUESTRA
SEÑORA DE BELEN DE CÚCUTA

LEIDY YOANA BAYONA MORENO
KATHERINE MEJIA TAMARA
BEATRIZ EUGENIA SARMIENTO CARVAJALINO

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
DIVISIÓN DE POSTGRADOS Y EDUCACIÓN CONTINUADA
ESPECIALIZACIÓN EN AUDITORIA EN SISTEMAS
OCAÑA
2014

CREACIÓN DE UN MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
PARA LA DEPENDENCIA SECRETARIA DE LA INSTITUCIÓN EDUCATIVA NUESTRA
SEÑORA DE BELEN DE CÚCUTA

LEIDY YOANA BAYONA MORENO
KATHERINE MEJIA TAMARA
BEATRIZ EUGENIA SARMIENTO CARVAJALINO

Trabajo de Grado presentado para optar al título de Especialista en Auditoria de Sistemas.

Director:
PhD (e). Mg. TORCOROMA VELÁSQUEZ
Ingeniera de Sistemas

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
DIVISIÓN DE POSTGRADOS Y EDUCACIÓN CONTINUADA
ESPECIALIZACIÓN EN AUDITORIA EN SISTEMAS
OCAÑA
2014

DEDICATORIA

A mi familia por ser el motivo que me impulsa para salir adelante, a mis compañeros de equipo por su acompañamiento y apoyo en cada una de las tareas realizadas, a las directivas de la Institución Educativa Nuestra Señora de Belén del Municipio de San José de Cúcuta, por creer en este proyecto y ayudarlo en su desarrollo, a la profesora Torcoroma Velásquez, al profesor Andrés Mauricio Puentes Velásquez por su decidido apoyo y confianza, a todos quienes conforman la comunidad educativa por trabajar de manera unida en la ruta de la calidad.

AGRADECIMIENTOS

Las autoras de este proyecto, presentan sus agradecimientos a:

La Msc. Torcoroma Velásquez, Directora del Proyecto, por su colaboración y valiosos conocimientos aportados al desarrollo del mismo.

La Universidad Francisco de Paula Santander Ocaña.

Todas aquellas personas, como los docentes y a nuestros padres que nos acompañaron, en el proceso de la carrera de ingeniería de sistemas y que de una u otra manera, nos ayudaron a la realización de este proyecto.

TABLA DE CONTENIDO

	Pág.
INTRODUCCIÓN	13
1. CREACIÓN DE UN MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA DEPENDENCIA SECRETARIA DE LA INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN DE CÚCUTA.	14
1.1. PROBLEMA DE INVESTIGACIÓN.	14
1.1.1. Planteamiento del Problema.	14
1.1.2. Formulación del Problema.	14
1.2. OBJETIVOS.	15
1.2.1. Objetivo General.	15
1.2.2. Objetivos Específicos.	15
1.3. JUSTIFICACIÓN.	15
1.4. HIPÓTESIS.	16
1.5. DELIMITACIONES.	17
1.5.1. Delimitaciones Geográficas.	17
1.5.2. Delimitaciones Temporales.	17
1.5.3. Delimitaciones Conceptuales.	17
1.5.4. Delimitaciones Operativas.	17
2. MARCO REFERENCIAL.	18
2.1 MARCO HISTÓRICO.	18
2.1.1. Antecedentes Históricos Mundiales.	18
2.1.2. Antecedentes Históricos Nacionales.	19
2.1.3. Antecedentes Históricos Local.	20
2.2. MARCO CONCEPTUAL.	20
2.3. MARCO TEÓRICO.	23
2.4. ESTADO DEL ARTE.	24
2.5. MARCO LEGAL.	25
3. DISEÑO METODOLÓGICO.	29
3.1. TIPO DE INVESTIGACIÓN.	29
3.2. POBLACIÓN.	29
3.3. MUESTRA.	29
3.4. RECOLECCIÓN DE INFORMACIÓN.	29
3.5. ANÁLISIS DE INFORMACIÓN.	30

4. PRESENTACIÓN DE RESULTADOS.	31
4.1. DIAGNÓSTICO DE LA INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN.	31
4.1.1. Modelo De Objetivos.	31
4.1.1.1. Misión.	31
4.1.1.2. Visión.	31
4.1.1.3. Objetivos Institucionales.	31
4.1.1.4. Organigrama.	33
4.1.1.5. Filosofía.	33
4.1.1.6. Valores Institucionales.	34
4.1.1.6.1. La Persona.	34
4.1.1.6.2. Familia.	35
4.1.1.7. Sociedad y la convivencia ciudadana.	36
4.1.1.7.1. Sociedad.	36
4.1.1.7.2. Convivencia ciudadana	38
4.1.2. Modelo de responsabilidades.	38
4.2. ESTABLECER NORMAS SOBRE LOS PROTOCOLOS QUE PODRÍAN UTILIZARSE EN EL ÁREA DE LA SECRETARIA DE LA INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN DE CÚCUTA, BASADO EN LAS NORMAS INTERNACIONALES DE SEGURIDAD DE LA INFORMACIÓN Y DE DATOS.	54
4.3. DOCUMENTAR UN MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, QUE SE SUGIEREN PARA LA DEPENDENCIA SECRETARIA DE LA INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN DE CÚCUTA.	71
5. CONCLUSIONES	72
RECOMENDACIONES	73
REFERENCIAS BIBLIOGRÁFICAS.	74
ANEXOS	76

LISTA DE TABLAS

	Pág.
Tabla 1. Matriz DOFA	40

LISTA DE FIGURAS

	Pág.
Figura 1. Misión, Visión, Objetivos de La Institución Educativa Nuestra Señora de Belén	32
Figura 2. Organigrama de la Institución Educativa Nuestra Señora de Belén.	33
Figura 3. Diagrama de procesos	44
Figura 4. Diagrama de procesos matrícula	45
Figura 5. Diagrama de procesos calificación	46
Figura 6. Diagrama de subprocesos de matrícula	47
Figura 7. Diagrama de subprocesos de calificación	48
Figura 8. Diagrama de subproceso de inscripción	49
Figura 9. Descripción de subproceso de registro matrícula	50
Figura 10. Descripción de subproceso asignar salón	51
Figura 11. Descripción de subproceso ingreso de notas	52
Figura 12. Descripción subproceso registro notas-alumno	53

LISTA DE ANEXOS

	Pág.
ANEXO A. ENTREVISTA N° 01	77
ANEXO B. ENCUESTA N° 01	79
ANEXO C. LISTA DE CHEQUEO N° 01	83
ANEXO D. OBSERVACIÓN DIRECTA	91
ANEXO E. DICTAMEN	96
ANEXO F. DOCUMENTO DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	97
ANEXO G. RESULTADOS DE LA ENTREVISTA N° 01.	108
ANEXO H. RESULTADOS DE LISTA DE CHEQUEO.	113
ANEXO I. RESULTADOS DE OBSERVACION DIRECTA.	118

INTRODUCCIÓN

Desde el descubrimiento de la computadora en el siglo XX, hasta el momento; se han producido cambios en nuestra sociedad, cuya importancia sólo podemos percibir en estos momentos. Hoy en día, nuestro entorno está rodeado por las nuevas tecnologías, y a medida que transcurre el tiempo, estas avanzan sin límites y en ocasiones son utilizados incorrectamente provocando daños en el mismo sistema en el que han sido creados.

La seguridad en todas las empresas, es un factor imprescindible en todos los ámbitos profesionales y en la informática, es especialmente importante porque en los ordenadores es donde esta almacenada la información confidencial de una empresa. Por este motivo, es indudable el crecimiento de la importancia que tiene el procesamiento de la información en el funcionamiento de cualquier organización. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

Muchas empresas son amenazadas constantemente, en sus activos lo que pudiera representar miles o millones de pesos en pérdidas por esta causa. Las vulnerabilidades en los sistemas de información o en cualquier proceso que se llevan a cabo en las organizaciones, pueden representar problemas graves, por ellos es muy importante comprender los conceptos necesarios para combatirlos y defender los posibles ataques a la información.

Es por eso que la información es el objeto de mayor valor para las empresas. Por esto y otros motivos es un asunto tan importante para todos, pues afecta directamente a los negocios de una empresa o de un individuo. Hoy es imposible hablar de un sistema cien por cien seguros, sencillamente porque el costo de la seguridad total es muy alto. Por eso las empresas, en general, asumen riesgos: deben optar entre perder un negocio o arriesgarse a ser hackeadas. La cuestión es que, en algunas organizaciones puntuales, tener un sistema de seguridad muy acotado les impediría hacer más negocios.

El trabajo que se presenta a continuación, se encuentra enfocado a las Políticas de Seguridad Informática (PSI) de la Institución Educativa Nuestra Señora de Belén, que surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos. Estos permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

1. CREACIÓN DE UN MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA DEPENDENCIA SECRETARIA DE LA INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN DE CÚCUTA.

1.1. PROBLEMA DE INVESTIGACIÓN.

1.1.1. Planteamiento del Problema.

La Institución Educativa Nuestra Señora de Belén de Cúcuta, es un centro educativo de carácter oficial que ofrece los niveles de Educación formal básica y media técnica en convenio con el SENA, atiende a una población de estrato uno y dos, con bajos recursos económicos. Adicionalmente, es el centro educativo que posee mayor cantidad de alumnos en dicha ciudad y está integrada por cinco sedes; de las cuales las secretarías de la sede principal, son las encargadas de manejar toda la información del Establecimiento Educativo.

Debido a que todos los procesos se concentran en la secretaría de la Institución Educativa, se han presentado una serie de problemas con el manejo de la misma y esto se debe a que no tiene delineadas sus políticas de seguridad, esto es un punto crítico; ya que el flujo de la información que maneja de equipos informáticos, servicios, datos, y recursos humanos es extenso.

Esto conduce en una inadecuada administración de los recursos del establecimiento, que incurren en las posibles fallas de servicio, como por ejemplo:

- ✓ La pérdida de información,
- ✓ Información errónea,
- ✓ Información duplicada,
- ✓ No hay actualización de datos oportunamente,
- ✓ Y por último, Inconsistencia de información.

Lo cual conlleva a una mala toma de decisiones, dentro de la Institución Educativa, frente a futuros sucesos y la imagen que proyecta ante la comunidad no es la adecuada; ya que no existe un canal formal de comunicación; que indique, cual es el proceder a un determinado evento en relación con los recursos y los servicios que presta el establecimiento.

1.1.2. Formulación del Problema.

¿La creación del manual de políticas de seguridad de la información permitirá la protección de la misma contra la pérdida de confidencialidad, integridad o disponibilidad, tanto de forma

accidental como intencionada, al igual que garantizar la conservación y buen uso de los recursos informáticos con que cuenta la Institución Educativa Nuestra Señora de Belén?

1.2. OBJETIVOS.

1.2.1. Objetivo General.

Crear un manual de políticas de seguridad de la información para la dependencia secretaria de la Institución Educativa Nuestra Señora de Belén de Cúcuta.

1.2.2. Objetivos Específicos.

- ✓ Diagnosticar el estado de la seguridad de la información, de la dependencia de secretaria de la Institución Educativa Nuestra Señora de Belén de Cúcuta.
- ✓ Establecer normas sobre los protocolos que podrían utilizarse en el área de la secretaria de la Institución Educativa Nuestra Señora de Belén de Cúcuta, basado en las normas internacionales de seguridad de la información y de datos.
- ✓ Documentar por medio de un manual de políticas de seguridad de la información, que se sugieren para la dependencia secretaria de la Institución Educativa Nuestra Señora de Belén de Cúcuta.

1.3. JUSTIFICACIÓN.

“Actualmente hablar de la información es hablar de uno de los activos más importantes para las organizaciones -cualquiera que sea su negocio-, ya que ésta conduce y fija muchos de sus procesos críticos.”¹

Debido a las fallas que se han presentado en la Institución Educativa Nuestra Señora de Belén, se definió las políticas la seguridad de la información, para este centro educativo; ya que se han producido por el mal manejo de la información, afectando a las personas que trabajan en el plantel; y pues no se había visto como algo significativo, por lo que la problemática ha venido incrementando con el crecimiento del colegio. Con la creación de este manual se pone a disposición de sus trabajadores, profesores y estudiantes como herramientas que faciliten el desarrollo de sus funciones.

¹Disponible en: <http://www.icontec.org.co/index.php?section=208> 08/Agosto/2013 9:14pm

El manual de políticas de seguridad de la información para la dependencia de secretaría de la Institución Educativa Nuestra Señora de Belén, permitirá establecer las medidas o protocolos de seguridad de la información, en forma organizada, clara y concisa; para establecer la integridad, confidencialidad y disponibilidad de la información.

Las políticas y estándares de seguridad informática definidas en el manual, fueron establecidas como base a la protección de los recursos tecnológicos y de información. Además este documento se constituirá en una herramienta para mejorar las labores de supervisión y control de actividades y responsabilidades asignadas, el adiestramiento de nuevos empleados y la realización de auditorías por parte de los organismos competentes.

Cabe resaltar que la Institución Educativa, deberá establecer los mecanismos que considere necesario para verificar el cumplimiento de las políticas establecidas en este manual.

El presente manual representa, una herramienta de trabajo que se considera perfectible y susceptible a correcciones, por lo que se agradece a todos los miembros de la Institución, cualquier recomendación que contribuya a su enriquecimiento, la cual debe ser dirigida a la misma.

Unas de los beneficios es establecer y adoptar las políticas de la información establecidas en el documento, es porque estas son la base para la protección de los activos tecnológicos e información de la institución educativa; pero la solución a la problemática, que se presenta actualmente dentro de la Institución Educativa Nuestra Señora de Belén, corresponde únicamente al plantel como tal, ante la posibilidad continua de adopción, expansión y actualización del manual de políticas de seguridad de la información para la dependencia secretaria de dicho establecimiento; esto con el fin de minimizar los riesgos a los que están expuestos con respecto a la información.

1.4. HIPÓTESIS.

Con el diseño de las políticas de seguridad la Institución Educativa Nuestra Señora de Belén, tendrá un mayor control de la información que se maneja pues se minimizaran los riesgos de seguridad de la información dentro del centro educativo.

1.5. DELIMITACIONES.

1.5.1. Delimitaciones Geográficas.

El proyecto, será desarrollado en diferentes lugares; una parte presencial, donde se solicitará y con observación directa se recolectará toda la información de los procesos aplicando todas las encuestas y listas de chequeo correspondientes; se complementará con la parte virtual, para documentar las actividades designadas y posteriormente la creación del manual de políticas de seguridad para la Institución Educativa Nuestra Señora de Belén. Durante el proceso de investigación se llevará a cabo el estudio de normas y estándares inherentes a la seguridad de información y desarrollo de políticas

1.5.2. Delimitaciones Temporales.

El proyecto se desarrolló, en un tiempo máximo de 3 meses.

1.5.3. Delimitaciones Conceptuales.

Para tener claridad sobre los términos en que se enmarcará la creación del manual, se deben conocer los siguientes:

- ✓ Informática,
- ✓ Seguridad Informática,
- ✓ Seguridad Física,
- ✓ Tecnologías de Información,
- ✓ Políticas de seguridad de la información.

1.5.4. Delimitaciones Operativas.

Dentro de los obstáculos, que se podrían presentar para el desarrollo del proyecto, sería la disponibilidad de la institución, al solicitar los documentos requeridos a la misma y organizar la toda la información con la que cuentan, debido a las fallas que se vienen presentando actualmente.

2. MARCO REFERENCIAL.

2.1 MARCO HISTÓRICO.

El marco histórico presentado en esta sección se clasificará de la manera siguiente:

2.1.1. Antecedentes Históricos Mundiales.

El desarrollo de la ciencia y la tecnología, es uno de los factores más influyentes en la sociedad contemporánea, este sería imposible sin el avance de las fuerzas productivas, pues el desarrollo descansa sobre cimientos científicos tecnológicos.

Este adelanto científico – técnico de la sociedad en nuestros días, hace cada vez más compleja y necesaria, la información sirviendo esta para orientar la forma de proceder en la solución de problemas.

De esta manera, nos encontramos ante un nuevo paradigma de la empresa, en el que la medición del resultado económico no es el elemento central de la evaluación de su gestión. La evaluación del impacto, centra su análisis en los diferentes aspectos de la entidad: financiero, ambiente, producto, comunidad y el entorno en que actúa, recursos humanos, por medio de las líneas de diálogo establecidas con los grupos de interés.

Según importante doctrina, la Responsabilidad Social Empresaria (RSE) es un nuevo paradigma de gestión que comprende una visión del negocio a largo plazo y que incorpora valores como la ética, la transparencia y la responsabilidad en la toma de decisiones, integrándolos en su estrategia comercial y en sus actividades.

Por ello consideramos significativo que cada empresa tenga la capacidad de lograr en función de su cultura organizacional y de sus valores, una definición propia de responsabilidad social empresaria con el objetivo de contribuir a su desarrollo ambiental, económico y social de manera sustentable.

La responsabilidad que emerge excede al cumplimiento jurídico, pero no sustituye la legislación social, económica ni ambiental, ya que funciona como un sistema de responsabilidades compartidas entre los diferentes actores sociales que se encuentran involucrados.

De esta manera, en Argentina, se implementó un manual de políticas de seguridad de la información, que permite un mejor aprovechamiento de los recursos informáticos dentro de la universidad.

2.1.2. Antecedentes Históricos Nacionales.

En Colombia, el ICETEX consiente de las necesidades de las empresas, “En ICETEX la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de sus necesidades actuales, ICETEX implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.”²

Así mismo también se encuentran políticas de seguridad de la información para diferentes instituciones educativas dentro de ellas tenemos las siguientes:

Política para la Seguridad de la Información de la Universidad Distrital Francisco José de Caldas. Bogotá D.C., Colombia. En la actualidad la información de la institución se ha reconocido como un activo valioso y a medida que los sistemas de información apoyan cada vez más los procesos de misión crítica se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos. Nuestra institución, los sistemas y red de información enfrentan amenazas de seguridad que incluyen, entre muchas otras: el fraude por computadora, espionaje, sabotaje, vandalismo, fuego, robo e inundación. Las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso o ataques de denegación de servicio se hacen cada vez más comunes³.

Políticas de Seguridad de Activos de Información para la Universidad Tecnológica de Pereira. Pereira, Colombia. Presentar la posición de la institución frente a la protección de la información y dar lineamientos para mantener la disponibilidad de la información de acuerdo a las necesidades de continuidad planeadas a nivel de los procesos y por ende de la institución.

Esta guía define lineamientos que deberán seguirse al interior de la institución para el almacenamiento y recuperación de corto y largo plazo, así como de la recuperación de la información mantenida a nivel de medios de almacenamiento (cintas, discos ópticos, etc.) para responder a los requerimientos de los procesos de la institución. Estos lineamientos deberán ser

²Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior. Tomado de: <https://www.icetex.gov.co/dnnpro5/LinkClick.aspx?...0...> 10/Agosto/2013

³ UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS. Políticas para la Seguridad de la Información de la Universidad Distrital Francisco José de Caldas. Bogotá D.C., Colombia. 20h. [en línea]. http://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf

seguidos por todos los funcionarios y cada una de las direcciones involucradas en estas actividades⁴.

Dentro de la información recolectada, se demuestra que son muchas las empresas que están adoptando las políticas de seguridad de la Información; estas empresas son dedicadas especialmente a la prestación de servicios en la banca, educación superior, salud y fuerzas armadas del país. Sin embargo, todavía son muchas las empresas que requieren mejorar aspectos de seguridad por lo cual se deberá seguir trabajando sobre esta temática.

2.1.3. Antecedentes Históricos Local.

En Cúcuta, las empresas también se han venido afectando por esta problemática y se han venido desarrollando proyectos, en donde se estipulen las políticas de seguridad, aunque son pocas las que den cumplimiento a estos estándares.

Dentro de algunos proyectos que se desarrollaron, se encuentran:

- ✓ Lineamientos para una política de seguridad alimentaria y desarrollo regio local para la ciudad de Cúcuta.
- ✓ Manual de seguridad para la policía nacional.
- ✓ Modelo de seguridad de la información para la universidad libre.

En donde se evidenciaron fallas en cuanto a la seguridad física y lógica de la información.

2.2. MARCO CONCEPTUAL.

Amenaza informática.

Es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).

Análisis de riesgos.

Evaluación del posible impacto y probabilidad de materialización de las amenazas de seguridad a las que se encuentra expuesta una Organización. La finalidad es poder diseñar e implantar los controles de seguridad necesarios, establecer prioridades de implantación y reducir los riesgos existentes⁵.

⁴ UNIVERSIDAD TECNOLÓGICA DE PEREIRA. Políticas de Seguridad de Activos de Información. Pereira, Colombia. 18h. [en línea]. http://media.utp.edu.co/sistema-de-gestion-de-seguridad-de-la-informacion/archivos/politicas_sgsi.pdf

⁵MANUAL DE SEGURIDAD. [En línea]. [15 Mayo 2013]. Disponible En: https://euskadi.net/r47-contbp2z/es/contenidos/informacion/bp_segurtasuna/es_dit/adjuntos/MSPLATEA_c.pdf

Filtración de datos.

Sucede cuando se compromete un sistema, exponiendo la información a un entorno no confiable. Las filtraciones de datos a menudo son el resultado de ataques maliciosos, que tratan de adquirir información confidencial que puede utilizarse con fines delictivos o con otros fines malintencionados.

Ingeniería Social.

Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social.

Políticas.

Es el conjunto de grandes orientaciones y lineamientos que guían las acciones a desarrollar por la institución, a fin de mejorar su funcionamiento; directrices que se traducen en los objetivos y metas que un sistema se propone alcanzar dentro de un futuro determinado, asociados a la indicación de los medios más generales que deberán ser utilizados para alcanzarlos.

Plan de Políticas.

Conjunto coherente de políticas que cubre las actividades más sustantivas.

Procedimiento de seguridad.

Proporcionan las instrucciones detalladas para llevar a cabo las tareas relacionadas con la seguridad de la información. Los procedimientos tienen un ámbito reducido de actuación y tienen siempre carácter operativo. Los procedimientos complementan los estándares de seguridad aportando la operativa necesaria para cumplirlas⁶.

Política de seguridad.

Constituye las directrices básicas y duraderas de la seguridad de la información en una Organización. Estas directrices definen el marco de actuación de los siguientes niveles dentro del cuerpo normativo. Normalmente se trata de un documento breve y conciso que se toma como referencia para elaborar el resto del cuerpo normativo de seguridad⁷.

Seguridad de la Información.

Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas⁸.

⁶MANUAL DE SEGURIDAD. [En línea]. [15 Mayo 2013]. Disponible En: https://euskadi.net/r47-contbp2z/es/contenidos/informacion/bp_segurtasuna/es_dit/adjuntos/MSPLATEA_c.pdf

⁷MANUAL DE SEGURIDAD. [En línea]. [15 Mayo 2013]. Disponible En: https://euskadi.net/r47-contbp2z/es/contenidos/informacion/bp_segurtasuna/es_dit/adjuntos/MSPLATEA_c.pdf

⁸MANUAL DE SEGURIDAD. [En línea]. [15 Mayo 2013]. Disponible En https://euskadi.net/r47-contbp2z/es/contenidos/informacion/bp_segurtasuna/es_dit/adjuntos/MSPLATEA_c.pdf

Confidencialidad:

Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Disponibilidad:

Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Autenticidad:

Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Auditabilidad:

Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Protección a la duplicación:

Consiste en asegurar una transacción solo se realiza una vez, a menos que especifique lo contrario.

No repudio:

Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Legalidad:

Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

Confiabilidad de la información:

Que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Integridad:

Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Seguridad Física.

Consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Vector de ataque.

Es el método que utiliza una amenaza para atacar un sistema.

Vulnerabilidad.

Una debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas⁹.

Información:

Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

2.3. MARCO TEÓRICO.

Las políticas y los procedimientos de seguridad informática surgen como una herramienta organizacional para concienciar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información que favorecen el desarrollo y el buen funcionamiento de la organización. Deben considerarse como reglas a cumplir que surgen para evitar problemas y que se establecen para dar soporte a los mecanismos de seguridad implementados en los sistemas y en las redes de comunicación.

Un plan de seguridad en una organización debe estar soportado por políticas y procedimientos que definan porque proteger un recurso, que quiere hacer la organización para protegerlo y como debe procederse para poder lograrlo.

Una de los aspectos más importantes que se debe considerar, en el desarrollo de políticas de seguridad, es poder determinar qué es lo que se quiere proteger y de qué se quiere proteger. Para lograr esto es importante tener conocimiento de las vulnerabilidades y formas de ataque de los sistemas con que cuenta la organización.

Los ataques internos los pueden realizar personas con buen conocimiento de técnicas para acceder a cuentas a las que no están autorizados o pueden surgir como accidentes que se presentan por el mal uso de los recursos. Los ataques externos provienen de personas experimentadas en acceder a los sistemas a través de las diferentes modalidades en que las compañías se conectan a Internet. En general estas personas poseen buenos conocimientos sobre Software, Hardware, programación, Lenguaje Ensamblador, Sistemas Operativos, TCP/IP,

⁹MANUAL DE SEGURIDAD. [En línea]. [15Mayo 2013]. Disponible En https://euskadi.net/r47-contbp2z/es/contenidos/informacion/bp_segurtasuna/es_dit/adjuntos/MSPLATEA_c.pdf

protocolos de seguridad, etc. Algunos de estos son expertos en Ingeniería social, es decir que son capaces de engañar a los usuarios autorizados para que les terminen dando acceso a los sistemas. Algunas de las herramientas usadas por los atacantes se describen a continuación:

Sniffers

Un analizador de paquetes es un programa de captura de las tramas de una red de computadoras.

Es algo común que, por topología de red y necesidad material, el medio de transmisión (cable coaxial, cable de par trenzado, fibra óptica, etc.) sea compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él. Para conseguir esto el analizador pone la tarjeta de red en un estado conocido como "modo promiscuo" en el cual en la capa de enlace de datos no son descartadas las tramas no destinadas a la dirección MAC de la tarjeta; de esta manera se puede capturar (sniff, "olfatear") todo el tráfico que viaja por la red.

Programas de ocultamiento (zappers)

Son unos programas que borran las huellas de los ataques que se han hecho en los sistemas.

Crakeadores:

Herramientas que permiten averiguar las claves de un sistema aunque estén encriptados. Una de las herramientas más utilizadas en la prevención de ataques externos por parte de los intrusos de Internet (Hackers) es el Firewall que ofrece seguridad de protección contra intrusos determinando que servicios de la red pueden ser accedidos y quienes pueden utilizar estos recursos, manteniendo al margen a los usuarios no autorizados y en caso de una ataque genera alarmas de seguridad. La implementación de Firewalls debe soportarse dentro del marco de un sistema de gestión de seguridad de la información y debe ser respaldado por políticas de seguridad que definan las normas de acceso a la red.

Los Firewalls son una puerta de acceso entre el Internet y la red Interna, también pueden ser puertas de acceso entre diferentes subdivisiones de una red. Esta aplicación determina que paquete puede pasar y cual no. Puede operar a nivel de aplicación o sobre las capas de red o transporte.

2.4. ESTADO DEL ARTE.

Las organizaciones que requieren implementar una estrategia de seguridad para proteger su información bajo los estándares internacionales, deben desarrollar e implantar un SGSI (sistema de gestión de seguridad de la información). Este proceso de administración y certificación de seguridad se debe hacer según las normas ISO 17799/ BS-7799-2.

El estándar británico BS 7799-2 determina los requisitos para establecer y administrar un sistema de gestión de seguridad de la información (SGSI). Su primera versión sale en el año de 1995 como recomendaciones para seguridad basadas en las mejores prácticas, se hacen modificaciones a esta norma en los años 1998, 1999, 2001 y finalmente es actualizada en el año 2002 y corregida para convertirse en un estándar certificable aceptado actualmente por el ICONTEC en Colombia, aunque a la fecha no se conoce ninguna empresa certificada bajo este estándar en el país.

La norma ISO 17799:2000 contiene las recomendaciones para el aseguramiento de la información que se basan en las mejores prácticas de seguridad, esta norma es una evolución del estándar británico BS 7799 en su primera versión, no es certificable pero debe ser adoptado por las organizaciones que quieran obtener la certificación BS 7799-2:2002; cubre aspectos como el manejo de equipos, la administración de políticas, los recursos humanos y los aspectos legales entre otros. Esta norma se basa en 10 Dominios de control:

- ◆ Política de seguridad
- ◆ Organización de la seguridad
- ◆ Clasificación y control de recursos
- ◆ La seguridad del personal
- ◆ La seguridad física y ambiental.
- ◆ Administración de comunicaciones y operaciones
- ◆ Control de acceso
- ◆ Desarrollo y mantenimiento de sistemas
- ◆ Plan de continuidad del negocio
- ◆ Cumplimiento de normatividad legal

Cada dominio busca cumplir con unos objetivos que suman 56 en total. Para cumplir los objetivos se deben evaluar 127 controles que son las recomendaciones de la norma, las organizaciones deciden si adoptar o no el control dependiendo del nivel de seguridad que desean para sus activos informáticos.

2.5. MARCO LEGAL.

Dentro del marco vigente para las políticas de seguridad para las instituciones educativas se encuentran las siguientes:

LEYES INFORMÁTICAS COLOMBIANAS¹⁰.

- ✓ Ley estatutaria 1266 del 31 de diciembre de 2008. Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- ✓ Ley 1341 del 30 de julio de 2009. Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- ✓ Ley estatutaria 1581 de 2012. Entró en vigencia la Ley 1581 del 17 de octubre 2012 de **PROTECCIÓN DE DATOS PERSONALES**, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.
- ✓ Ley 603 de 2000. Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.
- ✓ La ley 1266 de 2008¹¹ y la ley 1273 de 2009¹², que afectan la seguridad de los datos.

Ley de derechos de autor¹³ expresa:

- ✓ Constitución política de 1991, en su artículo, que expresa: “El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley”.
- ✓ Decisión 351 de 1993 o Régimen común andino sobre derecho de Autor y derechos conexos, de aplicación directa y preferente a las leyes internas de cada país miembro del grupo andino.
- ✓ Ley 23 de 1982, contiene las disposiciones generales y especiales que regulan la protección del derecho de autor en Colombia.

¹⁰ UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Gerencia de Innovación y Desarrollo Tecnológico. Última actualización el Lunes, 22 de Abril de 2013 09:05. [en línea]. <http://www.unad.edu.co/gidt/index.php/leyesinformaticas>

¹¹ Disponible en: http://www.secretariassenado.gov.co/senado/basedoc/ley/2008/ley_1266_2008.html

¹² Disponible en: http://www.secretariassenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html

¹³ Ley 23 de 1982

- ✓ Ley 44 de 1993, modifica y adición a la Ley 23 de 1982.
- ✓ Decreto 460 de 1995, por la cual se reglamenta el Registro Nacional de Derecho de Autor.

Así mismo las normas ISO establecen:

- ✓ Como se puede ver en el primer capítulo, esta Ley está muy ligada a la ISO27000, lo cual coloca al País a la vanguardia en legislación de seguridad de la información, abriendo así la posibilidad de nuevas entradas con este tema.
- ✓ ISO/IEC 27001¹⁴ - es la certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005.
- ✓ ISO/IEC 27002 - Información tecnología - Security techniques - Code of practice for information security management. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es código de buenas prácticas para la gestión de seguridad de la información.
- ✓ Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007.
- ✓ ISO/IEC 27003 - son directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero del 2010, No está certificada actualmente.
- ✓ ISO/IEC 27004 - son métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre del 2009, no se encuentra traducida al español actualmente.
- ✓ ISO/IEC 27005 - trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada a la actual British Standard BS 7799 parte 3. Publicada en junio de 2008.
- ✓ ISO/IEC 27006:2007 - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma específica requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.

¹⁴Disponible en: <http://www.daminda.com/downloads/ISO27001.pdf>

- ✓ ISO/IEC 27007 - Es una guía para auditar al SGSI. Se encuentra en preparación.
- ✓ ISO/IEC 27799:2008 - Es una guía para implementar ISO/IEC 27002 en la industria de la salud.
- ✓ ISO/IEC 27035:2011 - Seguridad de la información – Técnicas de Seguridad – Gestión de Incidentes de Seguridad. Este estándar hace foco en las actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades.
- ✓ ISO 27000 y las normas ISO 27001, ISO 27002, ISO 27006 e ISO 27799.

3. DISEÑO METODOLÓGICO.

3.1. TIPO DE INVESTIGACIÓN.

El tipo de investigación planteada para esta indagación, es “la investigación descriptiva cuyo propósito es especificar las propiedades, características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a un análisis “(Danhke, 1989).

La investigación descriptiva se desarrollará, debido a que se requiere información del área, en ella podemos obtener datos más profundos acerca de la problemática anteriormente dicha.

Posteriormente, se analizará toda la información obtenida durante la investigación, para plantear una solución al problema planteado.

3.2. POBLACIÓN.

La población a la que se le realizará, la propuesta investigativa será al área de la secretaria de la Institución Educativa Nuestra Señora de Belén de Cúcuta, conformada por las secretarías del establecimiento, ya que ahí es el sitio, donde se realizan todas las operaciones del plantel educativo. También se tomarán referencias de algunos datos suministrados por el cuerpo docente.

3.3. MUESTRA.

Para la muestra de la investigación se tomó el 100% de la población y fue sujeto al método empírico o subjetivo

3.4. RECOLECCIÓN DE INFORMACIÓN.

Se hará uso de las siguientes técnicas para la recolección de información:

- ✓ Entrevista,
- ✓ Lista de chequeo,

- ✓ Cuestionario,
- ✓ Observación directa
- ✓ Y pruebas de cumplimiento.

3.5. ANÁLISIS DE INFORMACIÓN.

Para el análisis de la información, se tomó como base el resultado de los diferentes métodos de recolección de información (ver ANEXO A, ANEXO B, ANEXO C, ANEXO D).

Adicionalmente se muestran los resultados de los métodos de recolección de la información aplicados a las siguientes personas:

- ✓ Rector
- ✓ Secretarias
- ✓ Docentes.

Para ver los resultados de las encuestas realizadas, se pueden ver en forma detallada en: ANEXO G, ANEXO H, ANEXO I.

Por lo general se estableció, que el mayor medio de comunicación que hay entre los profesores y la institución educativa es la página web, aunque cuentan con fallas en cuanto a la seguridad de los procesos y de la información que se manejan dentro de la institución. También se evidencia la falta de direccionamiento estratégico que encamine hacia la calidad de un buen manejo de los lineamientos institucionales.

4. PRESENTACIÓN DE RESULTADOS.

4.1. DIAGNÓSTICO DE LA INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN.

A continuación se presenta el sistema actual con el que cuenta la Institución Educativa Nuestra Señora de Belén.

4.1.1. Modelo De Objetivos.

El diagrama de objetivos presenta la jerarquía de los objetivos, desde el objetivo global hasta los proyectos y programas planeados, para llevarlos concretamente a la práctica. El diagrama de objetivos es de utilidad para la formulación de las preguntas de evaluación. Ofrecen una visión sintética de la estrategia propuesta en los documentos oficiales.

4.1.1.1. Misión.

La Institución Educativa “Nuestra Señora de Belén”, busca formar niños(as) y jóvenes con principios éticos, sociales y culturales fundamentados en estrategias administrativas y pedagógicas que posibiliten proyectar un ciudadano con calidades humanas, capaz de enfrentar al mundo laboral y productivo, mejorando progresivamente su vida y el desarrollo de la comunidad.

4.1.1.2. Visión.

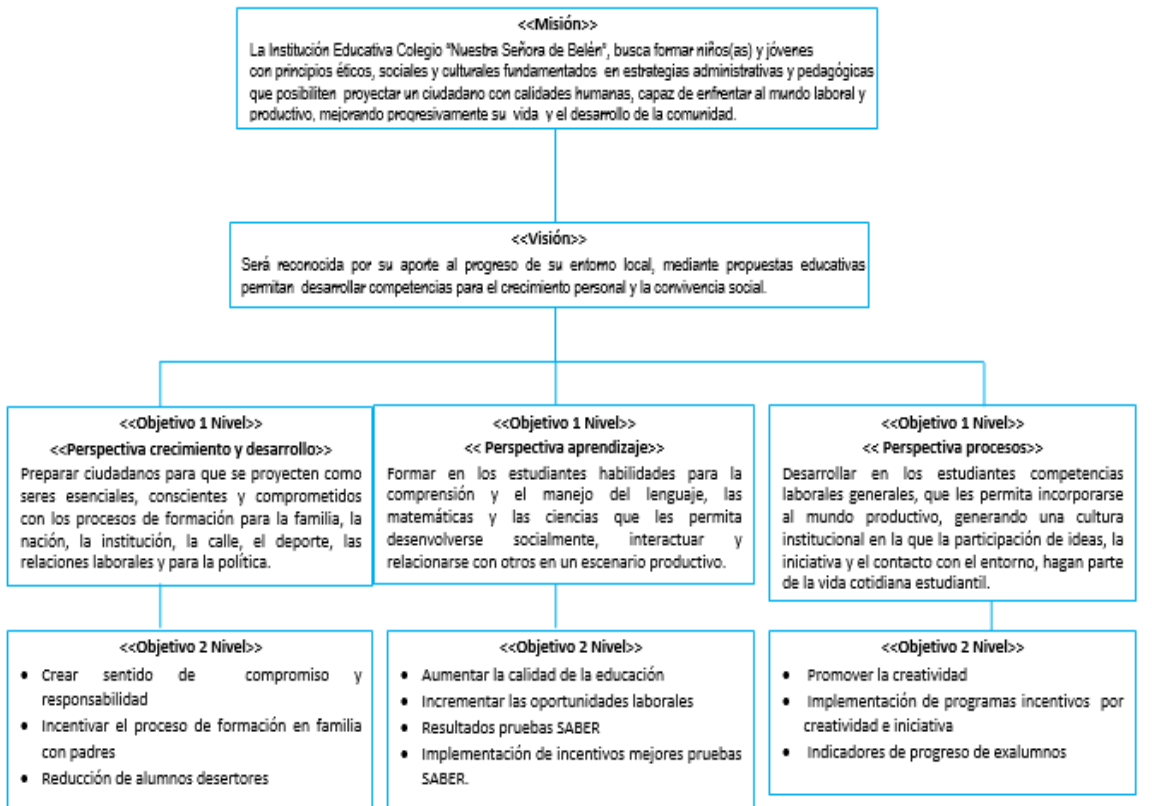
En año 2020, la Institución Educativa "Nuestra Señora de Belén del municipio de San José de Cúcuta, será reconocida por su aporte al progreso de su entorno local, mediante propuestas educativas que permitan desarrollar competencias para el crecimiento personal y la convivencia social.

4.1.1.3. Objetivos Institucionales.

- ✓ Formar hombres y mujeres con alta sensibilidad humana y social, comprometidos con el progreso y la convivencia de la institución, con el fin de poseerla como una de las mejores en la ciudad de San José de Cúcuta en el nivel Técnico.
- ✓ Desarrollar programas pedagógicos que favorezcan la cultura de la ciencia, el arte, la tecnología, la producción y la ecología, formando ciudadanos competentes capaces de enfrentarse al mundo del trabajo.
- ✓ Integrar a la comunidad Educativa para que participe en los diferentes procesos que exige el desarrollo del Proyecto Educativo Institucional.

- ✓ Liderar programas de formación permanente con los docentes, para que innoven pedagógica y tecnológicamente en el aula, buscando que los estudiantes desarrollen los aprendizajes que requieren para ser competentes en el mundo del trabajo.
- ✓ Formar en los estudiantes habilidades para la comprensión y el manejo del lenguaje, las matemáticas y las ciencias que les permita desenvolverse socialmente, interactuar y relacionarse con otros en un escenario productivo.
- ✓ Preparar ciudadanos para que se proyecten como seres esenciales, conscientes y comprometidos con los procesos de formación para la familia, la nación, la institución, la calle, el deporte, las relaciones laborales y para la política.

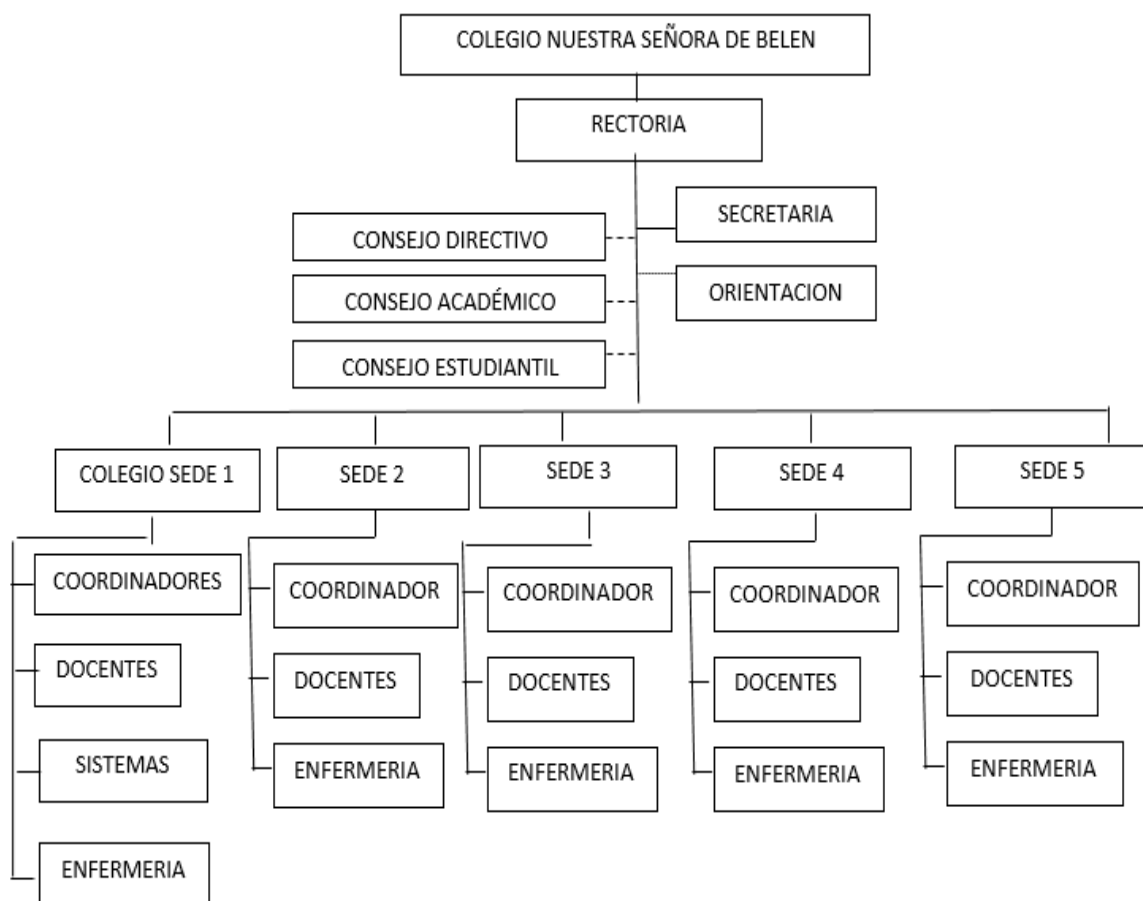
Figura 1. Misión, Visión, Objetivos de La Institución Educativa Nuestra Señora de Belén



Fuente: Autores del proyecto

4.1.1.4. Organigrama.

Figura 2. Organigrama de la Institución Educativa Nuestra Señora de Belén.



Fuente: Autores del proyecto

4.1.1.5. Filosofía.

La comunidad educativa Colegio Nuestra señora de Belén se rige por los principios de la educación colombiana, consagrados en la Constitución Política de 1991 y la Ley General de Educación (Ley 115 de 1994), los cuales indican que “la educación es un proceso de formación permanente, personal, cultural y social que se fundamenta en una concepción integral de la persona humana, de su dignidad, de sus derechos y sus deberes”. Y cuya finalidad está expresada en el artículo 5 de la Ley 115 de 1994, de conformidad con el artículo 67 de la Constitución Política.

Nuestra acción educativa está encaminada al desarrollo de competencias básicas, generales y específicas en procura del crecimiento personal y la convivencia social, para ello, se propone e implementa procesos de mejoramiento pedagógico que: exalta y dignifica la persona, genera el amor por el conocimiento, la ciencia y la tecnología, fortalece la armonía social y mejora la calidad de vida introduciendo al educando al mundo productivo.

La propuesta pedagógica busca ser pertinente de acuerdo a la realidad económica, social, política y cultural de nuestro entorno y contexto; encaminada a lograr la formación integral de la persona en procesos de pensamiento, aprendizaje y socialización, en saberes, valores y competencias fundamentales para la construcción de una comunidad con capacidad de autogestión y participación activa en la satisfacción de sus necesidades.

El educando es reconocido como el motor de la labor educativa, pues es el autor de su desarrollo dimensional: corporal, cognoscitivo, ético, estético, espiritual y volitivo; donde el propósito es la interiorización de conocimientos significativos que favorezcan el pleno desarrollo de su personalidad, la capacidad para la toma de decisiones, el trabajo en equipo, el uso creativo de los recursos y el tiempo libre, el manejo y solución de problemas y conflictos, el respeto por el medio y ante todo el desarrollo responsable de su proyecto de vida.

4.1.1.6. Valores Institucionales.

Los valores humanos son acciones conscientes y voluntarias, en las que se hace uso de la libertad para obrar correctamente reconociendo la dignidad de la persona humana.

Los valores Institucionales son los principios que orientan el quehacer pedagógico generando un clima de trabajo con el fin de darle coherencia, unidad y sentido a la acción educativa.

Para la comunidad educativa Nuestra Señora de Belén, los valores fundamentales están categorizado en:

4.1.1.6.1. La Persona.

Para la institución Educativa Colegio “Nuestra Señora de Belén”, el estudiante debe ser persona capaz de formarse mostrando actitudes coherentes con su dignidad, construir su propio destino y su historia, desarrollar su propio criterio en la búsqueda la verdad y no ser manipulado por otros, querer el bien por voluntad propia y no por obligación, afrontar las dificultades con confianza y optimismo, demostrando autoestima y deseos de superarse para mejorar la sociedad en que vive. Para esto se requiere:

- ✓ Forma auténticas personas que procuren el progreso y adelanto de una institución, región y de un país, para desarrollarse y crecer dentro del compartir en la vida.
- ✓ Asumir el reto de comprometerse decididamente con la transformación de la historia y con la construcción de un mundo mejor, asumiendo el cambio como un deber personal.

- ✓ Reconocer sus diferencias individuales, que le permitan proyectarse como un ser social con capacidades de enfrentarse al mundo laboral y social afrontando los retos del mundo cambiante.
- ✓ Aprender a descubrir que es un ser pensante y libre, capaz de tomar sus propias decisiones y de asumir con responsabilidad las consecuencias de las mismas.
- ✓ Identificar su propia dignidad, libertad y responsabilidad para encontrar el camino a la realización personal, a su actitud de apertura permanente al cambio y al progreso, contribuyendo profundamente en la transformación de la sociedad.

4.1.1.6.2. Familia.

La familia: comunidad de personas creadas sobre el sólido fundamento del amor y no puede realizarse nada pedagógicamente sino a través del amor. El vínculo de la sangre debe dar paso a otros vínculos más espirituales: el respeto, el amor, la felicidad, el disfrutar de la vida juntos, el ayudarse. Nuestros hijos nos brindan cada día y a cada momento la oportunidad de convertirnos en los padres que hubiéramos querido tener. Para la Comunidad Educativa Nuestra Señora de Belén los valores que requiere la familia son:

- ✓ RESPETO.- Trátale como si ya fuera tan buena persona como tú quisieras que sea; dejar que el otro sea él mismo.
- ✓ AMOR.- Como algo permanente. Un niño necesita la seguridad en el amor para tener confianza en sí mismo.
- ✓ HONRADEZ.- Que los demás puedan confiar en nosotros.
- ✓ VALENTÍA Y VALOR.- Tesón, saber encarar las cosas, afrontar las dificultades. En la medida en que estás haciendo lo que no te gusta pero te conviene, en esa medida te estás formando.
- ✓ ESPERANZA.- Actitud mental positiva, creer en lo que se está haciendo.
- ✓ GENEROSIDAD.- Deseos de hacer el bien, de salir de uno mismo, de ayudar a los demás.
- ✓ DAR SENTIDO A LA VIDA.- Espiritualidad, mete a Dios en tu vida.
- ✓ LA SAGACIDAD.- Estar bien despiertos y descubrir las alarmas de la sociedad: la droga...

4.1.1.7. Sociedad y la convivencia ciudadana.

4.1.1.7.1. Sociedad.

La sociedad es la responsable y veedora de la educación con la familia y el Estado. La sociedad debe colaborar en la vigilancia de la prestación del servicio educativo y en el cumplimiento de su función social. Los valores que la sociedad debe aportar a nuestra juventud son:

✓ Autodominio.

Formar un carácter capaz de dominar la comodidad y los impulsos propios de su forma de ser para hacer la vida más amable a los demás.

✓ Decencia.

El valor que nos recuerda la importancia de vivir y comportarse dignamente en todo lugar.

✓ Sensibilidad.

Es el valor que nos hace despertar hacia la realidad, descubriendo todo aquello que afecta en mayor o menor grado al desarrollo personal, familiar y social.

✓ Comunicación.

Una buena comunicación puede hacer la diferencia entre una vida feliz o una vida llena de problemas.

✓ Compasión.

La compasión se enfoca en descubrir a las personas, sus necesidades y padecimientos, con una actitud permanente de servicio.

✓ Orden.

A todos nos agrada encontrar las cosas en su lugar, pero lo más importante es el orden interior y es el que más impacta a la vida.

✓ Servicio.

Brindar ayuda de manera espontánea en los detalles más pequeños, habla de nuestro alto sentido

de colaboración para hacer la vida más ligera a los demás.

✓ Amistad.

Elemento primordial para salir adelante cuando sientes que el mundo se te viene encima.

✓ Honestidad.

La honestidad es una de las cualidades que nos gustaría encontrar en las personas o mejor aún, que nos gustaría poseer.

✓ Solidaridad.

Un valor que nos ayuda a ser una mejor sociedad y que no solo debe vivirse en casos de desastre y emergencia.

✓ Patriotismo.

El valor que nos hace vivir plenamente nuestro compromiso como ciudadanos y fomentar el respeto que debemos a nuestra nación.

✓ Liderazgo.

Todo líder tiene el compromiso y la obligación de velar por la superación personal, profesional y espiritual de quienes lo rodean. Es una responsabilidad que como personas debemos asumir.

✓ Superación.

La superación no llega con el tiempo, el simple deseo o con la auto motivación, requiere acciones inmediatas, planeación, esfuerzo y trabajo continuo.

✓ Autoestima.

No basta tener seguridad en nuestras capacidades, el valor de la autoestima está fundamentado en un profundo conocimiento de nosotros mismos.

✓ Compromiso.

Comprometerse va más allá de cumplir con una obligación, es poner en juego nuestras capacidades para sacar adelante todo aquello que se nos ha confiado.

✓ Responsabilidad

4.1.1.7.2. Convivencia ciudadana

La convivencia ciudadana es tener conciencia social de responsabilidad, es reconocer el valor de las personas y de las cosas, y darles el debido trato. Es reconocer los principios básicos de urbanidad y civismo, para brindar a los demás la acogida a partir de los buenos modales, la cortesía y la amabilidad. Todos los miembros de la institución han de aportar su creatividad, sus iniciativas, su sentido común, su actitud de servicio y empeño constante por construir la verdadera fraternidad que hace posible la convivencia social. Para lograr la convivencia se debe:

- ✓ Aprender a no agredir al congénere.
- ✓ Aprender a Comunicarse.
- ✓ Aprender a interactuar.
- ✓ Aprender a decidir en grupo.
- ✓ Aprender a cuidarse.
- ✓ Aprender a cuidar el entorno.
- ✓ Aprender a valorar el saber social.

PRODUCTIVIDAD

Entendida como la capacidad de todo individuo de utilizar el conocimiento y sus habilidades individuales para producir bienes y servicios que contribuyan a proporcionarle bienestar personal y social; y valorar la práctica del trabajo como una opción dignificante para los seres humanos. Esto implica:

- ✓ Solución de problemas.
- ✓ La excelencia.
- ✓ La calidad.
- ✓ El liderazgo.
- ✓ Trabajar en equipo, para que pueda crear e innovar atendiendo las exigencias de la ciencia y la tecnología.
- ✓ Investigar permanentemente sobre las necesidades y demandas sociales y de la comunidad.
- ✓ Pro actividad: Mantener una actitud de cambio permanente.
- ✓ Gestionar recursos.

4.1.2. Modelo de responsabilidades.

Dentro del modelo de responsabilidades, de la Institución Educativa Nuestra Señora De Belén de Cúcuta encontramos los siguientes actores con sus respectivas responsabilidades dentro de la oficina

SECRETARIA

- ✓ Expedir los certificados que sean solicitados por las Estudiantes y Padres de Familia.
- ✓ Colaborar con la organización y ejecución del proceso de matrículas.
- ✓ Suministrar a Coordinación Académica las planillas de calificaciones.
- ✓ Llevar la hoja de vida y documentación de los Docentes actualizándola a comienzos de año.
- ✓ Organizar la documentación de las Estudiantes y llevar los correspondientes registros académicos.
- ✓ Inscribir anualmente a la Institución en la oficina correspondiente, presentando los datos estadísticos.
- ✓ Revisar y registrar anualmente la documentación de las Estudiantes de Undécimo Grado, elaborando las actas correspondientes.
- ✓ Imprimir Boletines bimestrales y finales de las Estudiantes de acuerdo con lo establecido para este fin por las Directivas del Colegio.
- ✓ Atender debidamente al público en las horas señaladas por el Colegio.

Matriz DOFA

OPORTUNIDADES

- Dispone de tecnología para el manejo de la información de alumnos y docentes.
- Adquisición de nuevos elementos o herramientas tecnológicas.
- Actualmente en proceso de certificación ayuda de la secretaria brindando capacitación para dicho proceso.
- Alianzas estratégicas para el desarrollo de infraestructura e interacción y generación de nuevas ofertas en programas técnicos.
- Uso de las nuevas tendencias basadas en software libre para reducción de costos
- Aprovechar los medios publicitarios para atraer nuevos alumnos.

FORTALEZAS

- Es el colegio con mayor cobertura de la ciudad de Cúcuta.
- Personal capacitado en TIC.
- El trabajo realizado por algunos grupos de docentes en impulsar el uso de las TIC en el colegio.
- Poseen un software orientado a la web para tener la información más segura y confiable.

AMENAZAS

- Competencia con otras entidades con mejoramiento de planta física
- Competencia con otros entes educativos que ya están certificados.

- Ausencia de los funcionarios que apoyen al proceso de mejoramiento.
- Obsolescencia de los equipos informáticos.

DEBILIDADES

- Falta de medios con nuevas tecnologías (video, tableros electrónicos, video proyectores).
- Poca utilización de las TIC en el Aula de clase.
- Bajos resultados pruebas a la calidad de la educación.
- Las copias de seguridad de la información no están actualizadas ya que no se realiza de forma periódica sino al final del periodo o año escolar.

En el siguiente apartado se puede ver la matriz DOFA

Tabla 1. Matriz DOFA

	OPORTUNIDADES ESTRATÉGICAS	AMENAZAS ESTRATÉGICAS
ANÁLISIS EXTERNO	<ul style="list-style-type: none"> • Dispone de tecnología para el manejo de la información de alumnos y docentes. • Adquisición de nuevos elementos o herramientas tecnológicas. • Actualmente en proceso de certificación ayuda de la secretaria brindando capacitación para dicho proceso. 	<ul style="list-style-type: none"> • Competencia con otras entidades con mejoramiento de planta física • Competencia con otros entes educativos que ya están certificados. • Ausencia de los funcionarios que apoyen al proceso de mejoramiento. • Obsolescencia de los equipos informáticos
ANÁLISIS INTERNO	<ul style="list-style-type: none"> • Alianzas estratégicas para el desarrollo de infraestructura e interacción y generación de nuevas ofertas en programas técnicos. • Uso de las nuevas tendencias basadas en software libre para reducción de costos • Aprovechar los medios publicitarios para atraer nuevos alumnos. 	

**FORTALEZAS
DIFERENCIALES
BÁSICAS**

- Es el colegio con mayor cobertura de la ciudad de Cúcuta.
- Personal capacitado en TIC.
- El trabajo realizado por algunos grupos de docentes en impulsar el uso de las TIC en el colegio.
- Poseen un software orientado a la web para tener la información más segura y confiable.

ESTRATEGIAS FO

- Aprovechar las tecnologías utilizadas para adquirir mayor prestigio tanto a nivel regional como nacional
- Asegurar el posicionamiento de las institución para brindar un mejor servicio
- Expandir y mejorar las instalaciones
- Hacer periódicamente mantenimiento a los servidores y tecnologías utilizada para brindar un mejor servicio.
- Capacitaciones a docentes para mejorar resultados de pruebas de la calidad de la educación.
- Nuevos programas para promoción de bachilleres técnicos.

ESTRATEGIAS FA

- Mejorar la calidad de la educación los servicios desarrollando un programa de capacitación
- Realizar estrategias innovadoras como por ejemplo mejor docente del periodo académico, para comprometer a los docentes y brindar un mejor servicio
- Reestructuración de los contenidos de los planes de estudio para mejorar la calidad de la educación.

DEBILIDADES CRÍTICAS

Falta de medios con nuevas tecnologías (video, tableros electrónicos, video proyectores.
Poca utilización de las TIC en el Aula de clase.
Bajos resultados pruebas a la calidad de la educación.
Las copias de seguridad de la información no están

ESTRATEGIAS DO

- Realizar investigaciones de mercado para saber a qué empresas estarían dispuestas a donar equipos obsoletos.
- Aprovechar los medios publicitarios para atraer nuevos alumnos

ESTRATEGIAS DA

- Mejorar y dotar las instalaciones existentes para mejorar la calidad de la institución hablar con SENA para que estudiantes realicen sus prácticas.
- Las copias de seguridad de la información se deben realizar periódicamente al

actualizadas ya que no se realiza de forma periódica sino al final del periodo o año escolar.

- Consolidar a la Institución educativa como una entidad de una organización intachable.
- Capacitación a los padres de Familia de los estudiantes sobre el uso de la plataforma.
- Construcción de aulas de informática en cada sede.

final del periodo o año escolar.

- Capacitar a los docentes en la utilización de la plataforma Web colegios de tal manera que permita la colaboración y participación de los estudiantes en la construcción del conocimiento.

Fuente: Autores del proyecto

MODELADO DEL NEGOCIO

Para que la tecnología de información refleje los objetivos del negocio se requiere conocer el funcionamiento del negocio para ello necesita ser modelado. En este estudio se tomó como referencia el trabajo presentado con el método de modelado de negocio para desarrollo de sistemas de información (BMM) presentado por (Barrios &Montilva, 2005:2).

El modelado de negocios se define como un proceso de representación de uno o más aspectos o elementos de una empresa como el propósito, su estructura, funcionalidad, dinámica, lógica de negocios y componentes como fines, procesos, reglas, objetos, actores y unidades organizativas entre otras.

La empresa es una organización de negocios que puede ser visto como una actividad cuyas principales partes del sistema, llamados procesos de negocio son diseñados para llegar a un conjunto de objetivos previamente definidos. La ejecución de los procesos de negocio de la empresa se apoya normalmente en una especie de aplicación de software denominada Sistema de Información Empresarial (EIS).

Se puede definir el modelado de negocios como una herramienta conceptual que contiene un conjunto de objetos, conceptos y sus relaciones con el objetivo de expresar la lógica del negocio de una empresa (Osterwalder, Pigneur&Tucci, 2005:1). Proporciona una vista simplificada de la estructura de negocios que actúa como la base para la comunicación, mejoras o innovación y define los requisitos de los sistemas de información que apoyan la empresa (Ericsson &Penker, 2000:1).

En el desarrollo de software, los requisitos tienen lugar en el espacio de la solución; el modelado de negocios aporta información esencial para la ingeniería de requisitos.

En la ingeniería del negocio según el enfoque David Taylor, se aborda el problema de la divergencia entre los procesos de negocio y el software; en la idea de la ingeniería convergente el diseño del negocio es implementado directamente en el software y los dos diseños se convierten en dos facetas del mismo sistema, esto permite alinear el software a los procesos del negocio.

En el modelado empresarial se encuentra el enfoque Enterprise KnowledgeDevelopment EKD (Desarrollo de conocimiento empresarial), donde se provee una manera sistemática y controlada de analizar, entender, desarrollar y documentar una empresa y sus componentes.

En el enfoque Marshall, todos los aspectos de un negocio son modelados a través de cuatro conceptos relacionados: su propósito, procesos, entidades y organización; presenta los meta modelos de propósito y de procesos. El enfoque de Montilva y Barrios (Montilva& Barrios, 2004:1) integra diferentes aspectos en los enfoques anteriores. (Ver Figura 2.)

MÉTODO DE MODELADO DE NEGOCIOS (BMM)

Método de modelado de negocios orientado al desarrollo de sistemas de información empresarial se fundamenta en: la noción de sistema de negocios (Montilva, 2002), el método EKD EKD-CMM CMM (Barrios & Nurcan, 2004:1) y el Método WATCH (Montilva& Barrios, 2004:2) para desarrollo de software empresarial.

El producto principal del método BMM (Ver Figura 3) es un modelo del negocio fundamentado en el modelo conceptual de una empresa e incluye los siguientes modelos:

Modelo del producto. Descripción genérica del producto que produce el método: El modelo de negocios.

Un modelo de negocios es un documento compuesto de un conjunto de submodelos; cada uno describe uno o más elementos organizacionales mediante diagramas UML Y BPMN, y estos submodelos constan de un conjunto de diagramas UML 2.0, UML Business y BPMN.

MODELO DE PROCESO.

Representación gráfica de las fases, pasos, actividades o tareas que el método propone para modelar el negocio.

El modelo del proceso BMM describe las actividades que el Grupo de Modelado debe seguir para elaborar el Modelo de Negocios. Es iterativo y versionado, asegura la calidad del modelo a través de la verificación y validación (V&V).

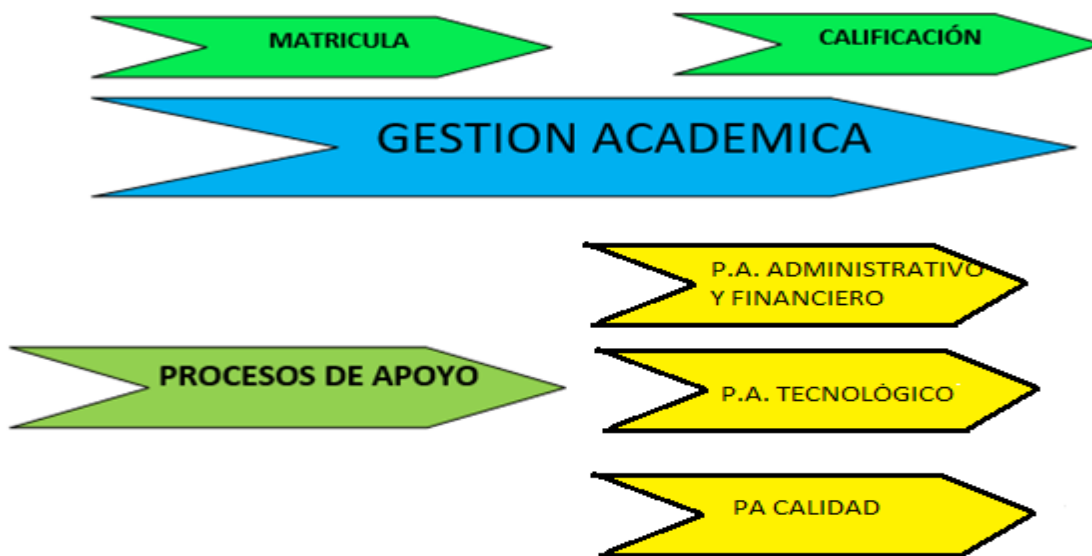
DIAGRAMA DE PROCESOS

El diagrama de procesos es una forma gráfica de presentar las actividades involucradas en la elaboración de un bien y/o servicio terminado, mostrando así el flujo de información. Cuenta con unas características entre las cuales están:

- ✓ Es cambiante, se adapta a la realidad de la empresa.
- ✓ Debe adecuarse a las especificaciones y necesidades de los clientes.
- ✓ Sirve como punto de control, para detectar posibles fallas.
- ✓ Debe ser medible.

A continuación se presenta el diagrama de procesos para la Institución Educativa Nuestra Señora de Belén, es una institución educativa, que presta sus servicios a la comunidad en general en el municipio de San José de Cúcuta.

Figura 3. Diagrama de procesos



Fuente: Autores del proyecto

La Institución Educativa Nuestra Señora de Belén cuenta con dos procesos fundamentales, que permiten cumplir con las exigencias establecidas en la organización, estos son:

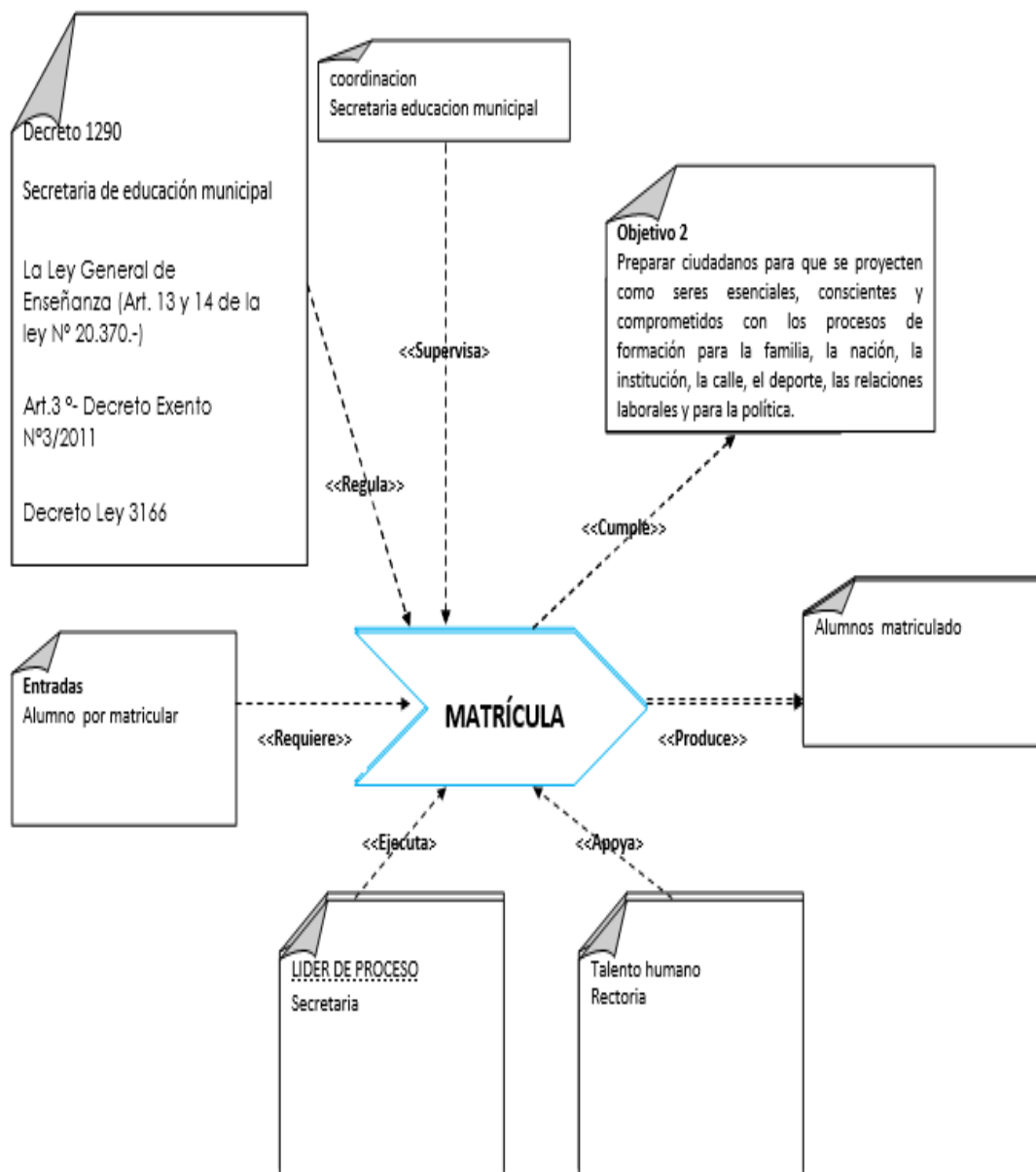
- ✓ PF Matricula
- ✓ PF Calificación

La descripción de cada uno de estos procesos representa en el Diagrama de Descripción de Procesos.

Diagrama de descripción de procesos

PF Matricula. El proceso fundamental de Gestión de Matricula, tiene como objetivo principal la matrícula de cada estudiante antiguo y nuevo dentro del centro educativo. Su descripción puede verse en la Figura 5.

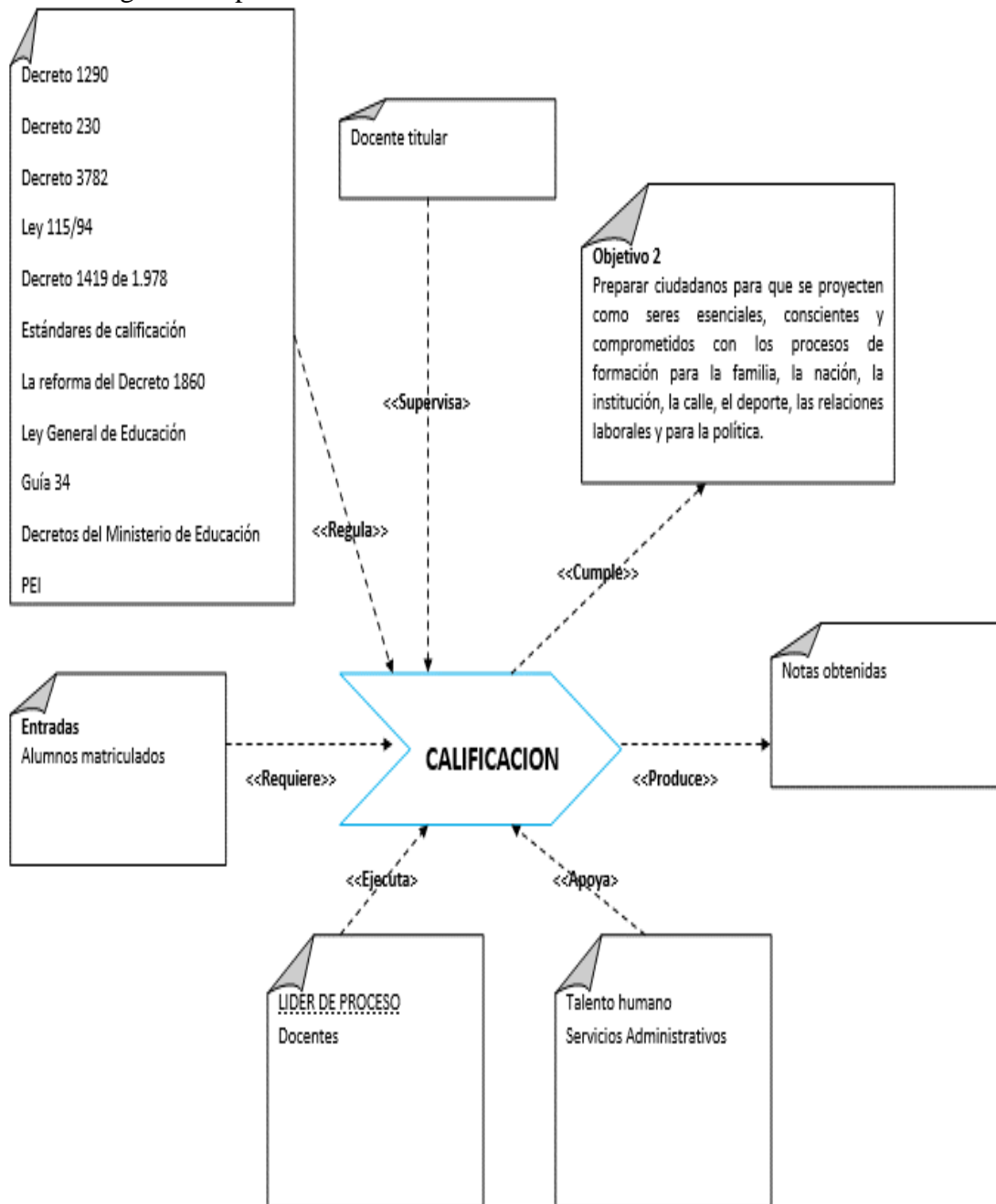
Figura 4. Diagrama de procesos matricula



Fuente: Autores del proyecto

PF Calificación. El proceso fundamental de Gestión de Calificación, tiene como objetivo principal la calificación de cada estudiante matriculado dentro del centro educativo. Su descripción puede verse en la Figura 6.

Figura 5. Diagrama de procesos calificación



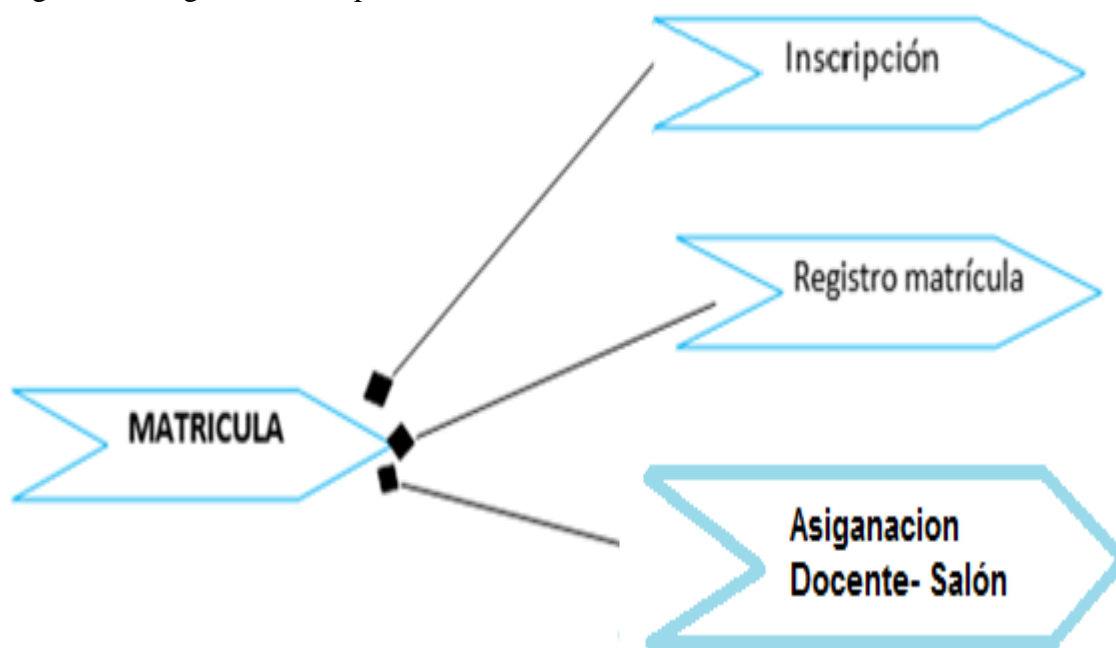
Fuente: Autores del proyecto

Así mismo, la descripción de subprocesos de PF Matricula, ilustrada en la figura 5 está compuesta por:

- ✓ Inscripción
- ✓ Registro matricula
- ✓ Asignación docente

Esta descripción de subprocesos se encuentra ilustrada en la figura 6

Figura 6. Diagrama de subprocesos de matricula



Fuente: Autores del proyecto

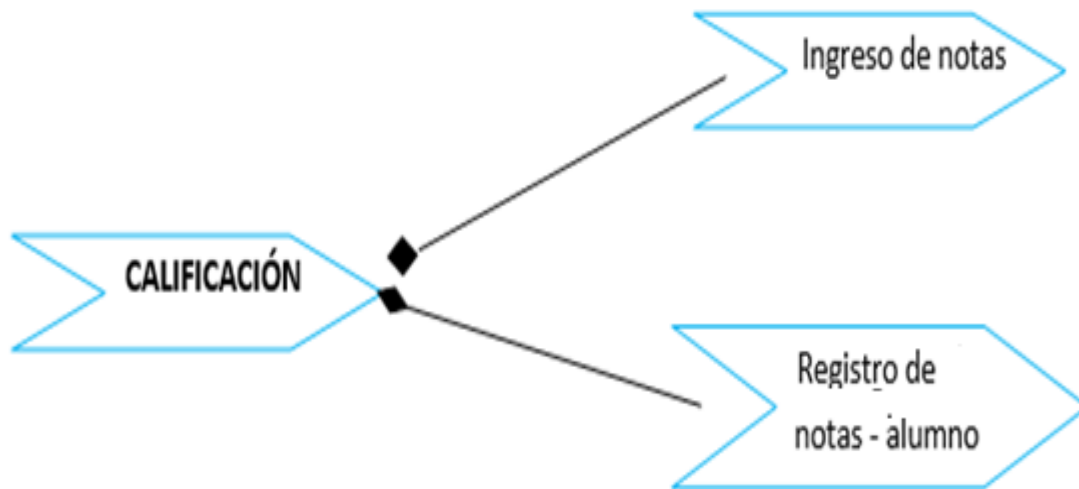
Inscripción: este subproceso se refiere principalmente el comienza del proceso de matrícula ya que el estudiante deberá primero tener una inscripción para que así la institución pueda seleccionarlos. Este se muestra en la figura 8

Registro matricula: este subproceso se refiere a que los estudiante de la institución después de matriculado ellos posean un registro de matrícula para así ingresarlos a la base de datos. Este se muestra en la figura 9

Asignación docente: este subproceso se refiere a que ya con un registro de matrícula ya empieza la institución a tomar decisiones internamente sobre el estudiante. Este se muestra en la figura 10

De la misma manera, la descripción de subprocesos de PF Calificación, ilustrada en la figura 6 está compuesta por:

Figura 7. Diagrama de subprocesos de calificación



Fuente: Autores del proyecto

Ingreso de notas: este subproceso se refiere que la institución hace una entrada las calificaciones de todos los estudiantes ya sea después de su periodo o su año lectivo para así darle salida de que se han ingresado las notas.

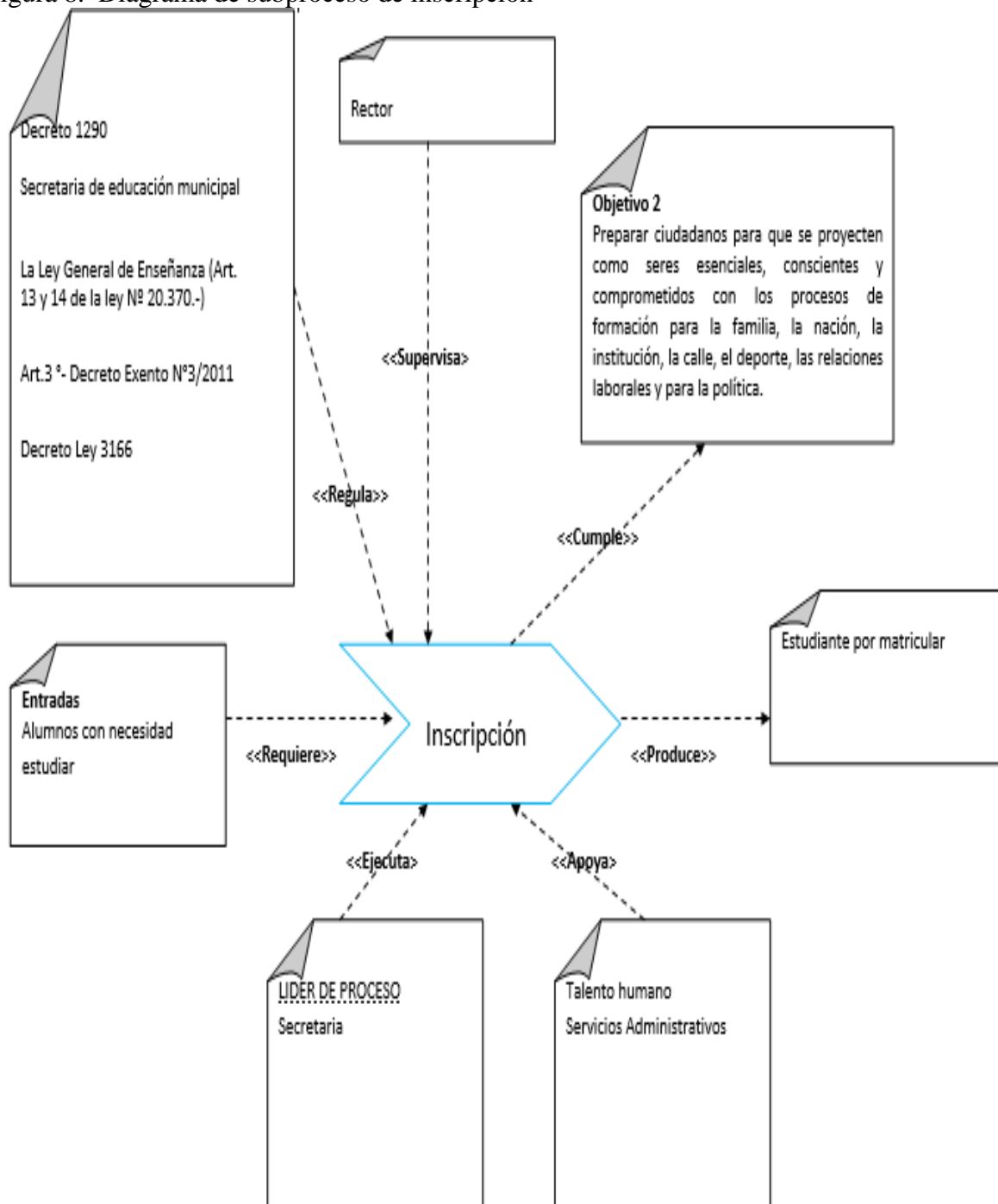
Registro de notas: este subproceso se refiere a que la institución después de ya allí notas ingresadas halla un registro para que así se definan que estudiante perdió materias o en caso del año lectivo aprobó o reprobó el año.

En la siguiente sección veremos las respectivas descripciones de cada subproceso

- Descripción de subproceso inscripción
- Descripción de subproceso registro matrícula
- Descripción de subproceso asignar docente salón
- Descripción de subproceso ingreso de notas
- Descripción subproceso registro notas – alumno

DESCRIPCION DE SUBPROCESO INSCRIPCION

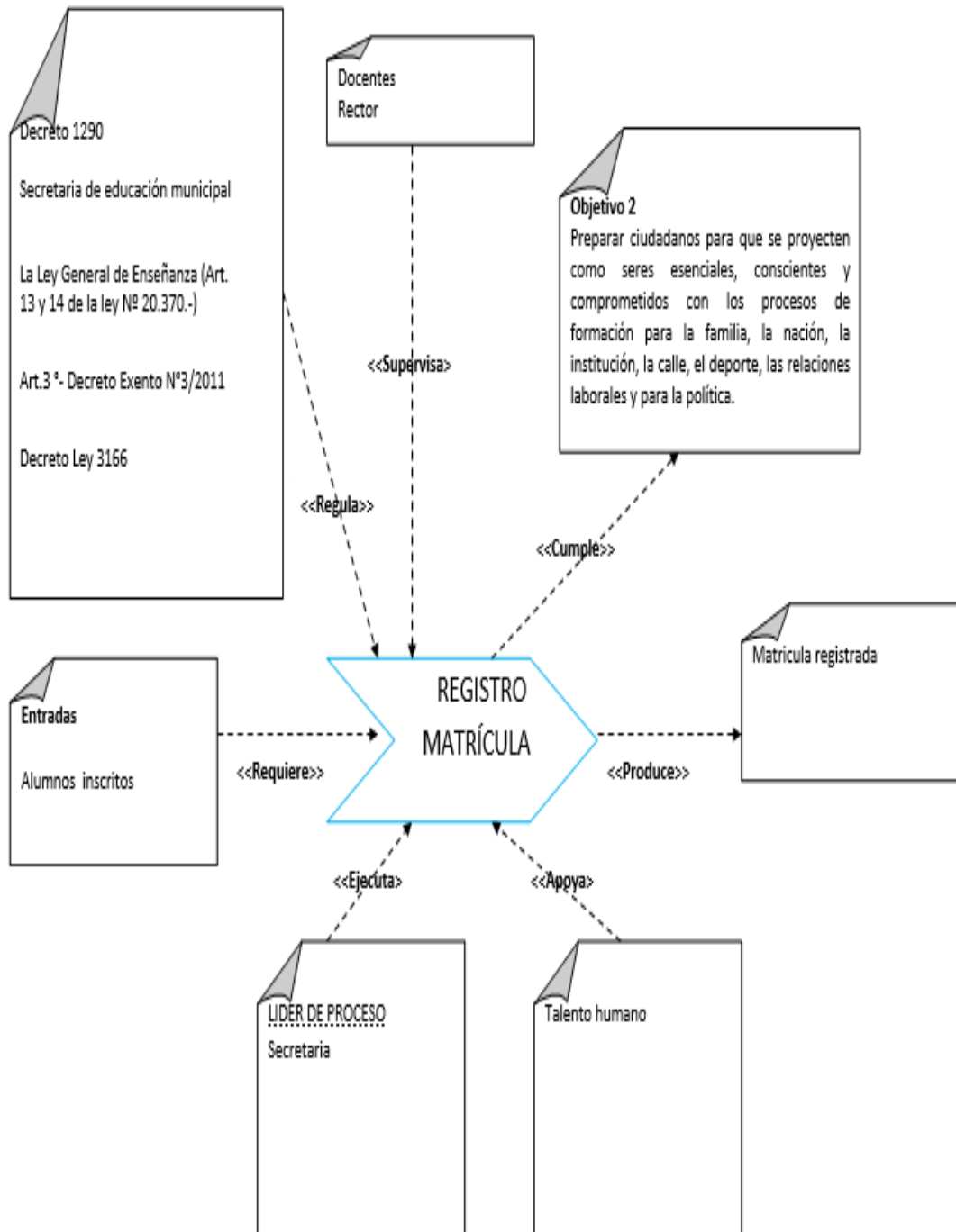
Figura 8. Diagrama de subproceso de inscripción



Fuente: Autores del proyecto

DESCRIPCION DE SUBPROCESO REGISTRO MATRÍCULA

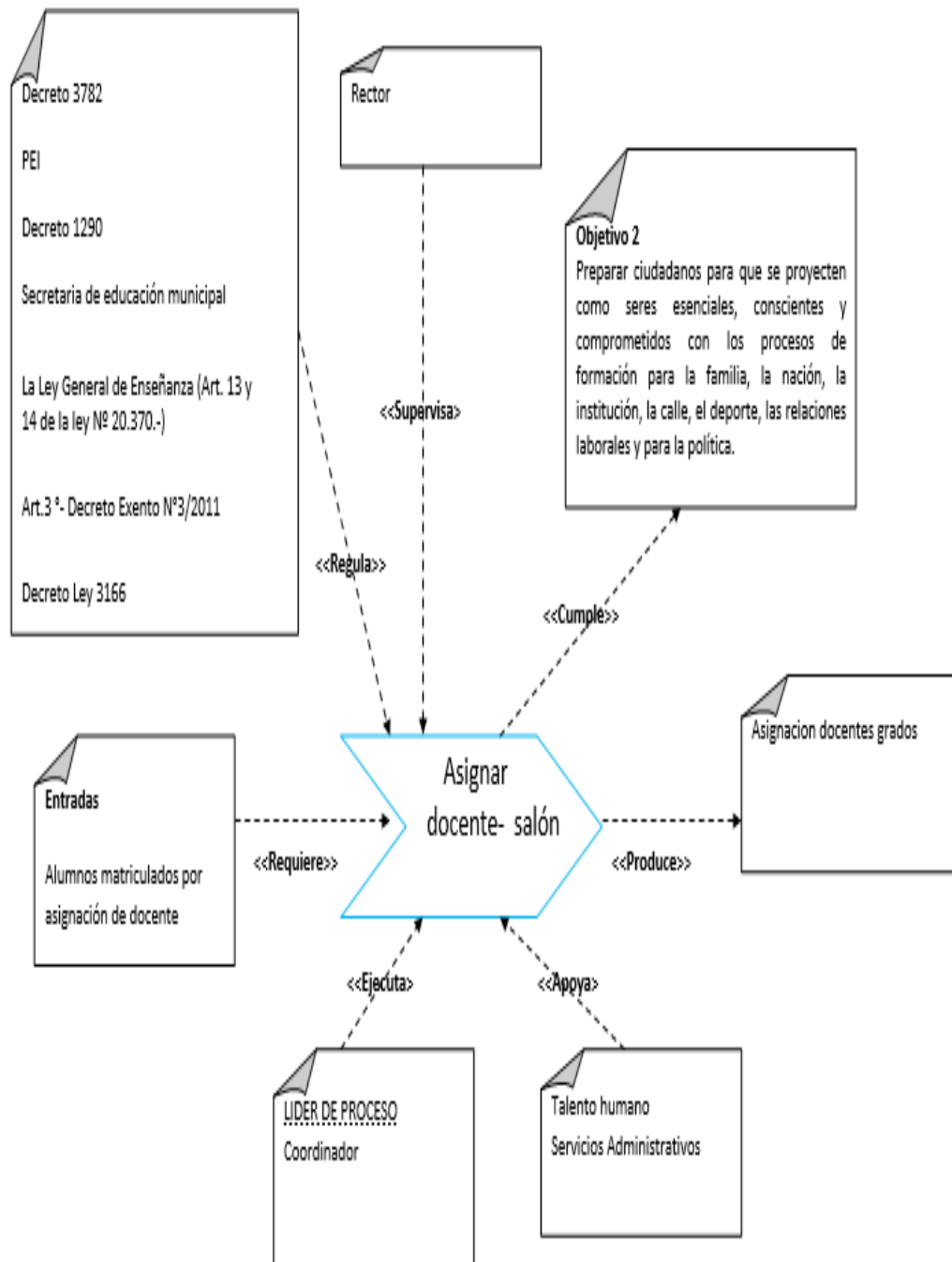
Figura 9. Descripción de subproceso de registro matricula



Fuente: Autores del proyecto

DESCRIPCION DE SUBPROCESOASIGNAR DOCENTE SALON

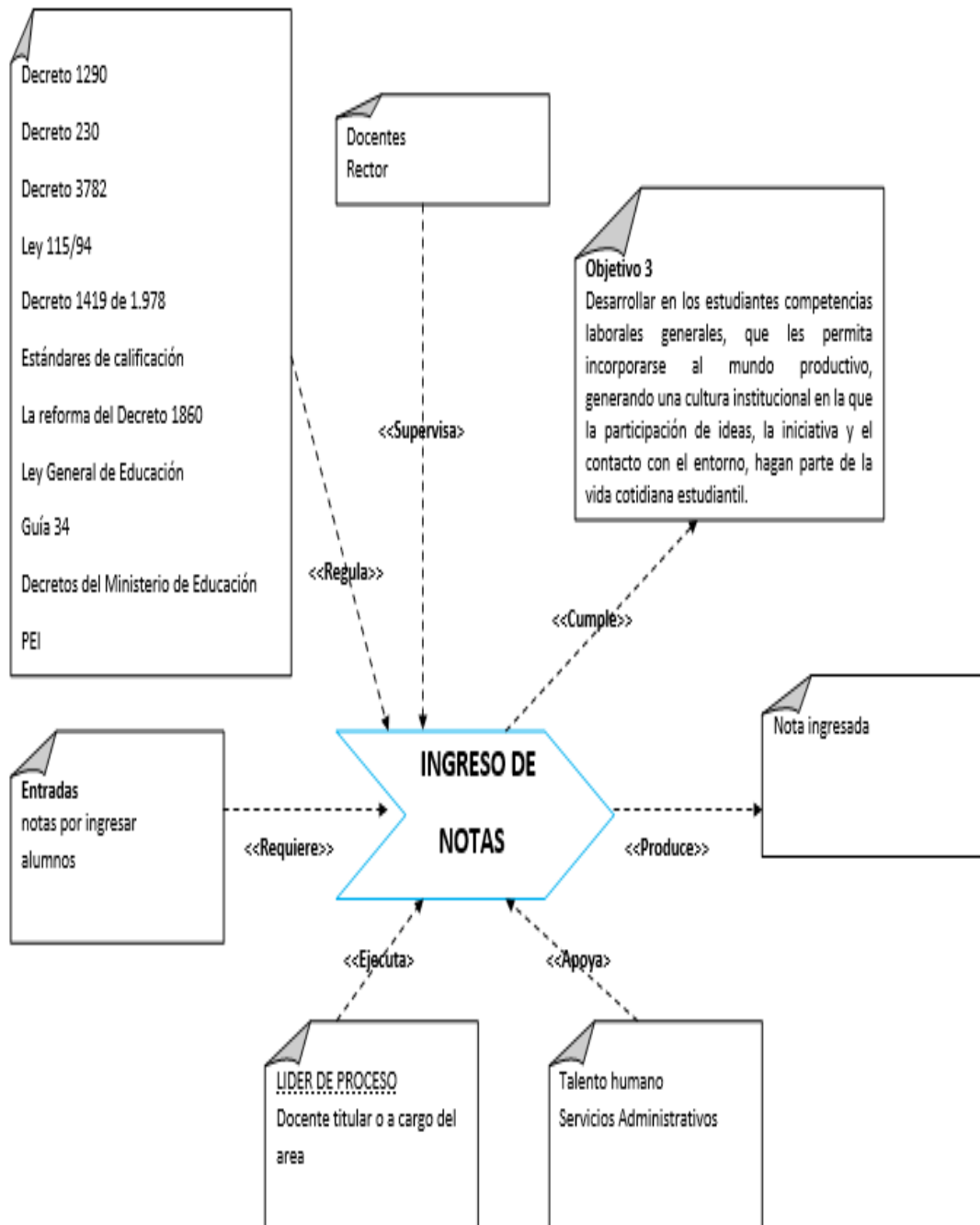
Figura 10. Descripción de subproceso asignar salón



Fuente: Autores del proyecto

DESCRIPCION DE SUBPROCESO INGRESO DE NOTAS

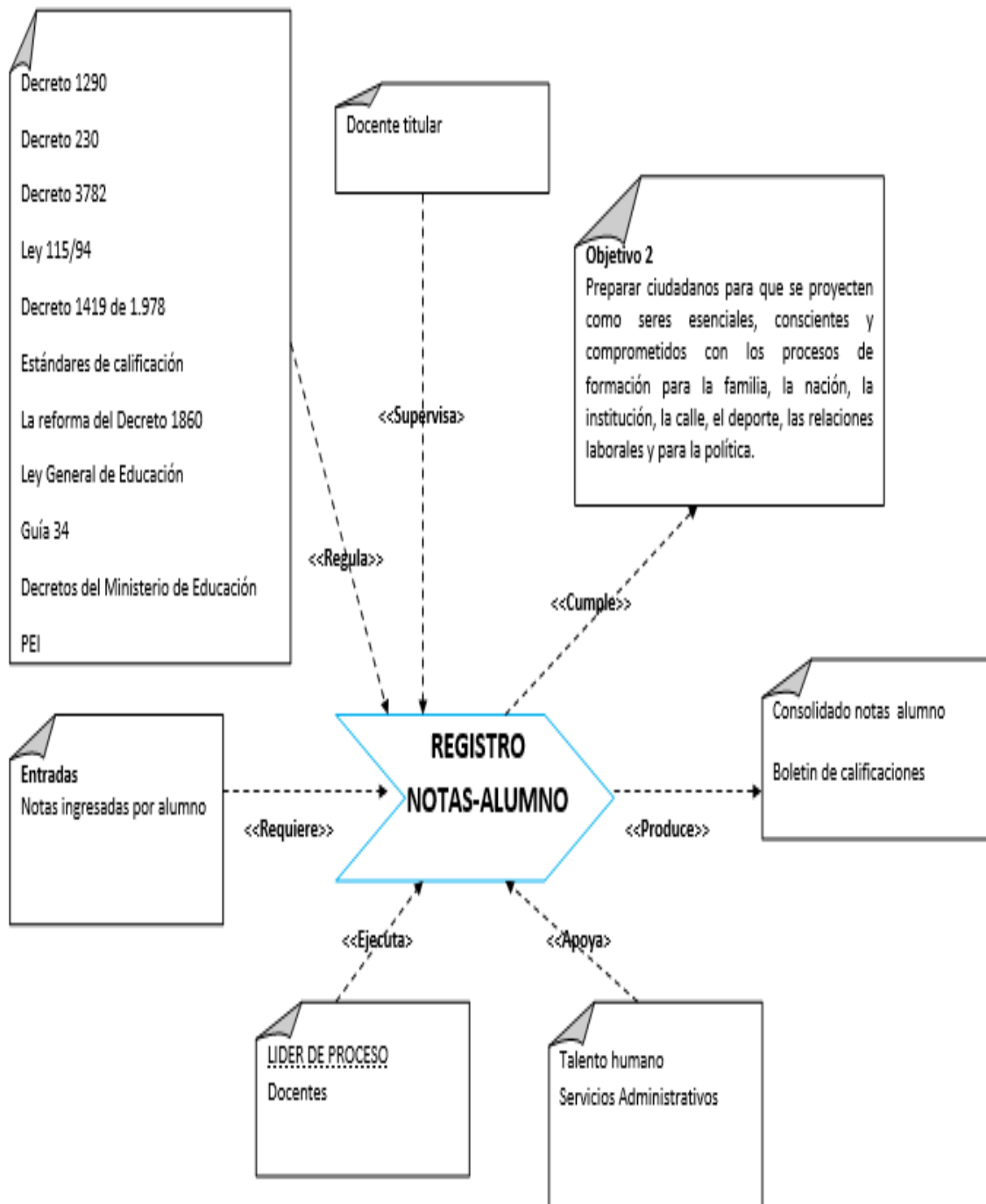
Figura 11. Descripción de subproceso ingreso de notas



Fuente: Autores del proyecto

DESCRIPCION SUBPROCESO REGISTRO NOTAS – ALUMNO

Figura 12. Descripción subproceso registro notas-alumno



Fuente: Autores del proyecto

Diagnóstico de la Institución Educativa Nuestra Señora de Belén.

La Institución Educativa, cuenta con una estructura definida, pero se encontraron varias debilidades y amenazas:

Falta de medios con nuevas tecnologías (video, tableros electrónicos, video proyectores.

- ✓ Las copias de seguridad de la información no están actualizadas ya que no se realiza de forma periódica sino al final del periodo o año escolar.
- ✓ Competencia con otras entidades con mejoramiento de planta física
- ✓ Competencia con otros entes educativos que ya están certificados.
- ✓ Ausencia de los funcionarios que apoyen al proceso de mejoramiento.
- ✓ Obsolescencia de los equipos informáticos.

4.2. ESTABLECER NORMAS SOBRE LOS PROTOCOLOS QUE PODRÍAN UTILIZARSE EN EL ÁREA DE LA SECRETARIA DE LA INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN DE CÚCUTA, BASADO EN LAS NORMAS INTERNACIONALES DE SEGURIDAD DE LA INFORMACIÓN Y DE DATOS.

Para establecer las normas sobre los protocolos que podrían utilizarse en el área de la secretaria de la Institución Educativa Nuestra Señora De Belén De Cúcuta, basado en las normas internacionales de seguridad de la información y de datos, se procedió a seguir los siguientes formatos descritos a continuación



RESUMEN DE DESVIACIONES DETECTADAS

EMPRESA	AREA AUDITADA	Día	Mes	Año
Institución Educativa Nuestra Señora de Belén	Secretaria	09	08	2013

REF	SITUACIONES	CAUSAS	SOLUCIÓN
	Desconocimiento de las responsabilidades y sanciones	No están establecidas las políticas de seguridad de la información.	Creación e implementación de un manual de políticas de seguridad de la información.
	Inconsistencia de información.	No están establecidas las políticas de seguridad de la información.	Creación e implementación de un manual de políticas de seguridad de la información.
	Se encuentra información duplicada.	No están establecidas las políticas de seguridad de la información.	Creación e implementación de un manual de políticas de seguridad de la información.
	Pérdida de información.	No están establecidas las políticas de seguridad de la información.	Creación e implementación de un manual de políticas de seguridad de la información.
	Información errónea	No están establecidas las políticas de seguridad de la información.	Creación e implementación de un manual de políticas de seguridad de la información.

Elaboró (nombre y firma)

Aprobó (nombre y firma)



RESUMEN DE SITUACIONES ENCONTRADAS

EMPRESA	AREA AUDITADA	Día	Mes	Año
Institución Educativa Nuestra Señora de Belén	Secretaria	09	08	2013

SITUACIONES	CAUSAS	SOLUCIÓN	FECHA SOLUCION	RESPONSABLE
Desconocimiento de las responsabilidades y sanciones	No están establecidas las políticas de seguridad de la información.	Creación e implementación de un manual de políticas de seguridad de la información		Rector Carlos Luis Villamizar Secretario Generales Lemny Andrea Aro Jaimes; Zoraida Parra Gómez; Diana Bethzabel Peláez Pineda
Inconsistencia de información.	No están establecidas las políticas de seguridad de la información.	Creación e implementación de un manual de políticas de seguridad de la información		Lemny Andrea Aro Jaimes; Zoraida Parra Gómez; Diana Bethzabel Peláez Pineda
Se encuentra información duplicada.	No están establecidas las políticas de seguridad de la información.	Creación e implementación de un manual de políticas de seguridad de la información		Lemny Andrea Aro Jaimes; Zoraida Parra Gómez; Diana Bethzabel Peláez Pineda

Elaboró (nombre y firma)

Aprobó (nombre y firma)

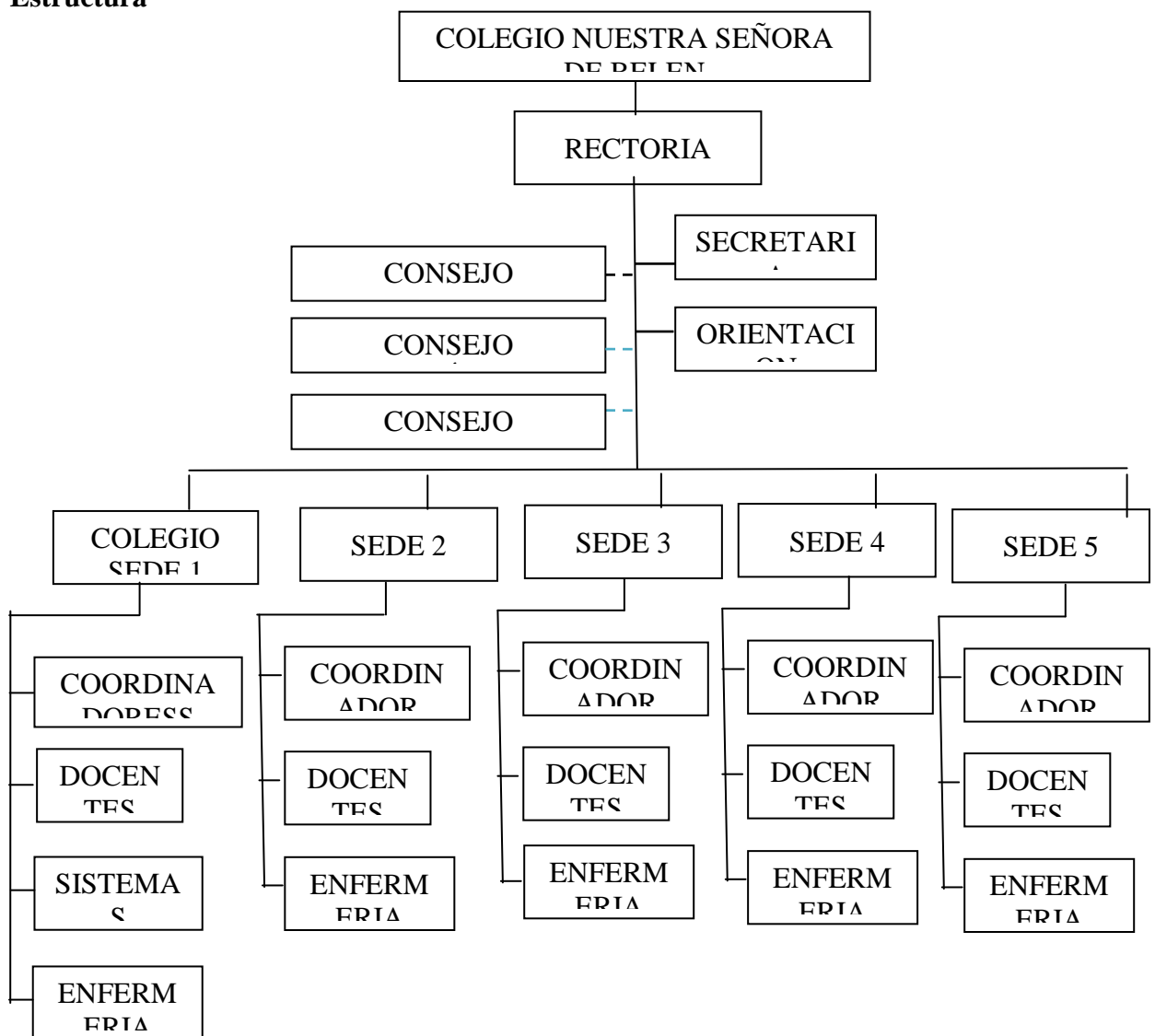
PROGRAMA GENERAL DE TRABAJO DE AUDITORÍA

DESCRIPCIÓN DE LA ENTIDAD AUDITADA

✓ Objetivo

Crear de un manual de políticas de seguridad de la información para la dependencia secretaria de la Institución Educativa Nuestra Señora de Belén de Cúcuta.

✓ Estructura



✓ **Sistemas**

Dentro de la Institución Educativa, el establecimiento cuenta con una sala de informática con 40 computadores para educar con acceso a Internet de 3 Megas de velocidad, los cuales son utilizados por los niños, docentes o cualquier persona que requiera este servicio. No cuenta como tal con una red que conecte estos computadores con el resto de computadores de la institución, por lo cual esto dificulta la comunicación entre ellos.

✓ **Otros**

Actualmente la Institución se encuentra en estado de remodelación y mejoramiento de la planta física por lo cual dificulta el normal funcionamiento de los procesos del colegio.

OBJETIVOS DE LA AUDITORÍA

✓ **Objetivos**

- Buscar una mejor relación costo-beneficio de los sistemas automáticos o computarizados diseñados e implantados.
- Incrementar la satisfacción de los usuarios de los sistemas computarizados.
- Asegurar una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles.
- Conocer la situación actual del área de secretaria y las actividades y esfuerzos necesarios para lograr los objetivos propuestos.
- Seguridad de personal, datos, hardware, software e instalaciones.
- Apoyo de función informática a las metas y objetivos de la organización.
- Seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático.
- Minimizar existencias de riesgos en el uso de Tecnología de información.
- Decisiones de inversión y gastos innecesarios.
- Capacitación y educación sobre controles en los Sistemas de Información.

✓ **Alcance del trabajo**

La auditoría se realizará en base al riesgo Fallas en los aplicativos, en el área de secretaria de la Institución Educativa Nuestra Señora de Belén de Cúcuta que permitirá analizar el manejo de la información que se manipula, teniendo en cuenta aspectos tales como la infraestructura, el diseño y niveles de seguridad.

DESCRIPCIÓN DE ÁREAS CRÍTICAS

En la Institución Educativa Nuestra Señora De Belén, el área crítica es la secretaria de dicho establecimiento. En esta área, se presentan muchas inconsistencias con respecto a la pérdida de información, manipulación de la información por personas con intenciones maliciosas, no disponibilidad y/o interrupción del procesamiento, ausencia de copias de seguridad, divulgación no autorizada de información, acceso no autorizado a las instalaciones, daño total o parcial de los equipos y retrasos, errores en la transmisión de información.

Cuenta con tres alimentadores del sistema de la plataforma Webcolegios:

- Lemny Andrea Aro Jaimes;
- Zoraida Parra Gómez;
- Diana Bethzabel Peláez Pineda

Se cuenta con tres computadores con acceso a internet cada uno con estabilizador y una UPS

PROGRAMAS DE AUDITORÍA

✓ Objetivos por área de control

AREA DE SECRETARIA

Participar en el desarrollo de nuevos sistemas:

Evaluación de controles

Cumplimiento de la metodología.

2. Evaluación de la seguridad en el área informática y de secretaria de la institución.

3. Evaluación de suficiencia en los planes de contingencia.

Respaldos, proveer qué va a pasar si se presentan fallas.

4. Opinión de la utilización de los recursos informáticos.

Resguardo y protección de activos.

5. Control de modificación a las aplicaciones existentes.

Fraudes

Control a las modificaciones de los programas.

6. Revisión de la utilización del sistema operativo y los programas

Utilitarios.

Control sobre la utilización de los sistemas operativos.

Programas utilitarios.

✓ **Procedimientos por área de control**

1. Expedir los certificados que sean solicitados por las Estudiantes y Padres de Familia.
2. Colaborar con la organización y ejecución del proceso de matrículas.
3. Suministrar a Coordinación Académica las planillas de calificaciones.
4. Llevar la hoja de vida y documentación de los Docentes actualizándola a comienzos de año.
5. Organizar la documentación de las Estudiantes y llevar los correspondientes registros académicos.
6. Inscribir anualmente a la Institución en la oficina correspondiente, presentando los datos estadísticos.
7. Revisar y registrar anualmente la documentación de las Estudiantes de Undécimo Grado, elaborando las actas correspondientes.
8. Imprimir Boletines bimestrales y finales de las Estudiantes de acuerdo con lo establecido para este fin por las Directivas del Colegio.
9. Atender debidamente al público en las horas señaladas por el Colegio.

RECURSOS NECESARIOS

✓ **Personal**

El proyecto será realizado por:

- Director del proyecto:
Torcoroma Velásquez.
- Investigadores:
LeidyYoana Bayona Moreno.
Beatriz Eugenia Sarmiento Carvajalino.
Katherine Mejía Tamara

✓ **Especialistas en el área.**

El proyecto será asesorado por la directora del proyecto Torcoroma Velásquez.

Así mismo contaremos con la asesoría de cada uno de los docentes de la especialización de auditoría de sistemas.

✓ **Presupuesto de tiempo**

La auditoría se llevara a cabo en el periodo comprendido entre el 14 de Junio al 14 de Agosto.

FAS E	DESCRIPCIÓN	ACTIVIDAD	NUM. PERSONAL PARTICIPANTE	PERIODO ESTIMADO		DÍAS HAB.	DÍAS HOM
				INICIO	TERMINO		
F01	Planeación	Preparación de herramienta	3	14 Julio	20 Julio	5	2
F02	Recopilación	Recolección de información	3	21 julio	28 julio	5	2
F03	Ejecución	Aplicación de pruebas	3	29 julio	14 agosto	18	2
F04	Culminación	Entrega de informe	3	15 agosto	16 agosto	2	2



GUIA DE AUDITORIA

EMPRESA
Institución Educativa Nuestra Señora de Belén

AREA AUDITADA
Secretaria

Día	Mes	Año
09	08	2013

Referencia	Actividad o función a evaluar	Procedimientos de auditoria	Herramientas que serán utilizadas	Observación
GA.01	Exploración del área a auditar	Examinar el espacio físico y lógico del área auditada.	Entrevista Observación	
GA.02	Solicitud de Información a la institución.	Solicitud de documentación manejada por el establecimiento	Revisión de los documentos	
GA.03	Recolección de Información	Elaboración y aplicación de herramientas de recolección de la información	Encuestas Entrevista Checklist Observación	
GA.04	Organización y análisis de la información Recolectada.	Organización de los papeles de Trabajo. Análisis de los resultados obtenidos de la auditoría realizada al área de secretaria	Entrevistas Documentación Cuestionario Listas de chequeo	



INVENTARIOS

Inventario de Software

EMPRESA		AREA AUDITADA		PERIODO			
Institución Educativa Nuestra Señora de Belén		Secretaria		DEL	09	08	2013
				AL	15	08	2013

Inventario de software, Equipo 001 (Secretaria general)

Ref.	Software	Versión	Núm. Inventario	Licencias	Presentación	Asignado a	Localización
SO.01	Windows XP	SP3	210-1	3	CD-DVD	Secretaria	Dpto.Secretaria
S.01	Office	2007	220-1	3	CD-DVD ROM	Secretaria	Dpto.Secretaria
S.02	Antivirus avast	8.0.1489		Free		Secretaria	Dpto.Secretaria
S.03	HP LaserJet Enterprise M4555h		235-2		CD-DVD ROM	Secretaria	Dpto.Secretaria
S.04	Nero 12	12.5.01300		Sin licencia		Secretaria	Dpto.Secretaria
S.05	Windows livemessenger			Free		Secretaria	Dpto.Secretaria

Inventario de software, Equipo 002 (Secretaria)

Ref.	Software	Versión	Núm. Inventario	Licencias	Presentación	Asignado A	Localización
SO.02	Windows XP	SP3	210-2	3	CD-DVD	Secretaria	Dpto.Secretaria
S.01	Office	2007	220-2	3	CD-DVD ROM	Secretaria	Dpto.Secretaria
S.02	Antivirus avast	8.0.1489		free		Secretaria	Dpto.Secretaria
S.03	HP LaserJet Enterprise M4555h		235-2		CD-DVD ROM	Secretaria	Dpto.Secretaria
S.04	Windows liveMessenger			free		Secretaria	Dpto.Secretaria

Inventario de software, Equipo 003 (Secretaria)

Ref.	Software	Versión	Núm. Inventario	Licencias	Presentación	Asignado A	Localización
SO.03	Windows XP	SP3	210-3	3	CD-DVD	Secretaria	Dpto.Secretaria
S.01	Office	2007	220-3	3	CD-DVD ROM	Secretaria	Dpto.Secretaria
S.02	Antivirus avast	8.0.1489		free		Secretaria	Dpto.Secretaria
S.03	HP LaserJet Enterprise M4555h		235-2		CD-DVD ROM	Secretaria	Dpto.Secretaria
S.04	Windows liveMessenger			free		Secretaria	Dpto.Secretaria



Inventario de hardware

EMPRESA
Institución Educativa Nuestra Señora de Belén

AREA AUDITADA
Secretaria

PERIODO			
DEL	09	08	2013
AL	15	08	2013

Inventario de hardware, Equipo 001 (Secretaria general)

Num.	Equipo	Marca	Num. Inventario	Características	Observaciones
1	Conexión de red	DSL		3 Mb	Conexión wifi
2	Computador	Samsung	C.235-1		Equipo de mesa
3	Procesador	Intel Pentium G645T		velocidad de 2,50GHz	
4	Disco duro			500GB	
	Pantalla LCD	Samsung	C.239	21,5"	
5	Memoria RAM			4 GB	
6	Estabilizador		C.230 - 4		
7	Impresora	HP Laserjet Enterprise M4555h	C.240	multifuncional	Compartida en red

Inventario de hardware, Equipo 002 (Secretaria)

Num.	Equipo	Marca	Num. Inventario	Características	Observaciones
1	Conexión de red	DSL		3 Mb	Conexión wifi
2	Computador	Samsung NP 300E4XA04	C.235-2		Computador portátil
3	Procesador	Intel Celeron B820			

4	Disco duro	SATA		500GB	
5	Memoria RAM	DDR3		4GB a 1.333MHz	
6	Estabilizador		C.230 – 2		
7	Impresora	HP Laserjet Enterprise M4555h		multifuncional	Compartida en red

Inventario de hardware, Equipo 003 (Secretaria)

Num.	Equipo	Marca	Num. Inventario	Características	Observaciones
1	Conexión de red	DSL		3 Mb	Conexión wifi
2	Computador	Lenovo	C.235-2		
3	Procesador	Intel Celeron 1007U		velocidad de 1.5 GHz	
4	Disco duro			500 GB	
5	Memoria RAM			4 GB	
6	Estabilizador		C.230- 5		
7	Impresora	HP Laserjet Enterprise M4555h		multifuncional	Compartida en red



REPORTE DE PRUEBAS

PRUEBA NO. 1	
INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN	
PRUEBA	Identificación de recursos, medidas de seguridad
OBJETIVO	Evaluar el nivel de seguridad informática de la Institución Educativa
TECNICA EMPLEADA	Entrevista
TIPO DE PRUEBA	Cumplimiento ___ Sustantiva ___ Doble finalidad <u>X</u>
PROCEDIMIENTO EMPLEAR	A 1. Realización de una entrevista al jefe de sistemas 2. Revisión de la entrevista realizada.
RECURSOS	Papel, lapicero
RESULTADOS DE LA PRUEBA	
HALLAZGOS	Los backup de la información desactualizada dado que no se realiza periódicamente
CAUSA	Falta de copias de seguridad actualizadas
SITUACIÓN DE RIESGO QUE GENERA	Información errónea o desactualizada
RECOMENDACIONES DE AUDITORIA	Guardar copias de seguridad en diferentes lugares y de manera periódica de manera que la información esté actualizada.
FECHA	09 – 08 – 2013
ELABORADO POR	LeidyYoana Bayona Moreno
REVISADA POR:	



PRUEBA No. 2 INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN	
PRUEBA	Revisión de los controles de acceso
OBJETIVO	Verificar el acceso a las aplicaciones y a los equipos de la secretaria
TECNICA EMPLEADA	Entrevista y observación
TIPO DE PRUEBA	Cumplimiento ___ Sustantiva ___ Doble finalidad <u>X</u>
PROCEDIMIENTO EMPLEAR	A 1. Realización de una encuesta al jefe de sistemas 2. Realización de una encuesta al personal que labora en el área de secretaria 3. Revisión de la encuesta realizada.
RECURSOS	Papel, lapicero
RESULTADOS DE LA PRUEBA	
HALLAZGOS	Las claves de acceso no se cambian de forma periódica y el lugar de trabajo ocupado con documentos, etc.
CAUSA	Desconocimiento de políticas de seguridad en el área de secretaria
SITUACIÓN DE RIESGO QUE GENERA	Acceso a la información por parte de personal ajeno a la institución
RECOMENDACIONES DE AUDITORIA	El lugar de trabajo se recomienda que este siempre despejado de modo que personal ajeno no acceda a la información y que se realice cambio de contraseña de acceso a los equipos de forma periódica, restringir que personal ajeno no tenga acceso al sitio de trabajo
FECHA	09 – 08 – 2013
ELABORADO POR	LeidyYoana Bayona Moreno
REVISADA POR:	



PRUEBA No. 3	
INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN	
PRUEBA	Revisión de las copias de seguridad
OBJETIVO	Comprobar si las copias de seguridad de la información se encuentran actualizadas
TECNICA EMPLEADA	Encuesta
TIPO DE PRUEBA	Cumplimiento ___ Sustantiva ___ Doble finalidad <u>X</u>
PROCEDIMIENTO EMPLEAR	A 1. Realización de una encuesta al jefe de sistemas 2. Realización de una encuesta al personal que labora en el área de secretaria 3. Revisión de la encuesta realizada.
RECURSOS	Papel, lapicero
RESULTADOS DE LA PRUEBA	
HALLAZGOS	Los backup de la información desactualizada dado que no se realiza periódicamente
CAUSA	Falta de realizar copias de seguridad de los datos de la Institución educativa
SITUACIÓN DE RIESGO QUE GENERA	Información errónea o desactualizada
RECOMENDACIONES DE AUDITORIA	Guardar copias de seguridad en diferentes lugares y de manera periódica de manera que la información este actualizada.
FECHA	09 – 08 – 2013
ELABORADO POR	LeidyYoana Bayona Moreno
REVISADA POR:	



PRUEBA No. 4	
INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN	
PRUEBA	Revisión de la documentación errónea.
OBJETIVO	Inspeccionar la veracidad, la consistencia y la integridad de los datos.
TECNICA EMPLEADA	Lista de chequeo
TIPO DE PRUEBA	Cumplimiento ___ Sustantiva ___ Doble finalidad <u>X</u>
PROCEDIMIENTO EMPLEAR	A 1. Realización de una encuesta al jefe de sistemas 2. Realización de una encuesta al personal que labora en el área de secretaria 3. Revisión de la encuesta realizada.
RECURSOS	Papel, lapicero
RESULTADOS DE LA PRUEBA	
HALLAZGOS	Información errónea, inconsistencia de información, se encuentra información duplicada y pérdida de información.
CAUSA	Falta explorar y organizar toda la información correspondiente.
SITUACIÓN DE RIESGO QUE GENERA	Información errónea, inconsistente, duplicada y perdida
RECOMENDACIONES DE AUDITORIA	Organizar y clasificar toda la información por semestre y año.
FECHA	12 – 08 – 2013
ELABORADO POR	LeidyYoana Bayona Moreno
REVISADA POR:	



PRUEBA No. 5 INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN	
PRUEBA	Revisión del perfil profesional
OBJETIVO	Comprobar si el perfil de cada persona que trabaja en el área de secretaria cumple con el perfil requerido.
TECNICA EMPLEADA	Encuesta
TIPO DE PRUEBA	Cumplimiento ___ Sustantiva ___ Doble finalidad <u>X</u>
PROCEDIMIENTO EMPLEAR	A 1. Realización de una encuesta al jefe de sistemas 2. Realización de una encuesta al personal que labora en el área de secretaria 3. Revisión de la encuesta realizada.
RECURSOS	Papel, lapicero
RESULTADOS DE LA PRUEBA	
HALLAZGOS	Personal no capacitado para esta área específica
CAUSA	Falta de conocimiento sobre determinados temas o de experiencia para laboral en el área.
SITUACIÓN DE RIESGO QUE GENERA	Información errónea, inconsistente, duplicada y perdida, ante la falta de experiencia o falta de conocimiento así mismo como retrasos.
RECOMENDACIONES DE AUDITORIA	Capacitar a las personal que se encuentra actualmente laborando o reasignar al personal que no cumple con los requisitos básicos requeridos para laborar en dicha área.
FECHA	09 – 08 – 2013
ELABORADO POR	LeidyYoana Bayona Moreno
REVISADA POR:	

4.3 DOCUMENTAR UN MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, QUE SE SUGIEREN PARA LA DEPENDENCIA SECRETARIA DE LA INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN DE CÚCUTA.

A partir del diagnóstico elaborado en la Institución Educativa Nuestra Señora de Belén y después de realizar el modelado del negocio para la institución se establecer el manual de políticas. (Ver Anexo F).

5. CONCLUSIONES

Lo primero y más importante es realizar el diagnóstico del estado de la seguridad de la información en este caso de la dependencia secretaria de la Institución Educativa Nuestra Señora de Belén de Cúcuta; pues éste, es el que nos ayuda a definir los riesgos que se presentan en el manejo de la misma, por lo que se deben utilizar diferentes herramientas de recolección de la información para su análisis y detectar todos los riesgos que se puedan presentar para dar solución.

Al establecer las Políticas de Seguridad basado en normas internacionales de seguridad de la información y de datos brindando solución y permitiendo control a los riesgos que se detectaron en el diagnóstico con las herramientas de recolección de información que se utilizaron, de manera que garantice la integridad, confidencialidad y disponibilidad de la misma.

Documentando por medio de la creación del manual de políticas de seguridad por lo que debe ser divulgado al personal, pues éste; servirá como una herramienta organizacional para concientizar a cada uno de los miembros de la Institución sobre la importancia y sensibilidad de la información y servicios críticos y de las fallas y riesgos que se pueden presentar por el mal manejo de la misma

RECOMENDACIONES

Colocar un límite de intentos al introducir la clave erróneamente porque esto se presta para que un usuario ajeno dé con la clave, acceda y haga modificaciones en la información.

Separación lógica y física, si es posible, de los datos y programas de explotación de aquellos datos y programas usados en desarrollo y mantención de sistemas.

Asignar (retirar) derechos y permisos sobre los ficheros y datos a los usuarios.

Crear una Política de Seguridad de la Información (PSI), que sea aprobada, distribuida y divulgada que todos la conozcan

Crear un Comité de Gestión de seguridad de la información y que todos lo conozcan.

Realización de pruebas de los planes de continuidad del funcionamiento del colegio para verificar si se puede contrarrestar las interrupciones que puedan presentar. (Sea por una falla eléctrica etc.)

Los mantenimientos de los equipos, soportes y datos, se realicen en presencia y bajo la supervisión de personal responsable y que en caso del traslado del equipo fuera de la entidad la información clasificada o limitada sea borrada físicamente o protegida su divulgación.

REFERENCIAS BIBLIOGRÁFICAS.

Anabalón, J. (2008). Desarrollo de métricas de seguridad SOX. ISSA. Documento en línea. Disponible en: http://anabalon.clan.su/papers/metricas_de_seguridad.pdf Consulta: 15/12/2009.

Cano, J. (2007). Métricas en seguridad informática: una revisión académica. VII Jornada de seguridad Informática ACIS. Documento en línea. Disponible en: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/07-MetricasSeguridadInformaticaUnaRevisionAcademica.pdf . Consulta: 27/02/2011.

Chalico, C. y Saucedo, E. (2008). Indicadores de gestión aplicados a los procesos de administración de riesgos y seguridad. Documento en línea. Disponible en: <http://ebookbrowse.com/6-chalico-saucedo-ppt-d59398282> . Consulta: 13/02/2009.

Chapin, D. y Akridg, S. (2005). ¿Cómo Puede Medirse la Seguridad? InformationSystems Control Journal. Volumen 2. Documento en línea. Disponible en: <http://www.iso27000.es/download/HowCanSecurityBeMeasured-SP.pdf> . Consulta: 15/10/2007.

Chew, E.; Swanson, M.; Stine, K.; Bartol, N.; Brown, A. & Robinson, W. (2008). Performance Measurement Guide for Information Security. Computer Security.NIST National Institute of Standars and Technology.Technology Administration U.S Department of Commerce.Documento en línea.Disponible en: <http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf> Consulta: 09/01/2009.

Corletti, A. y De Alba, C. (2008). Métricas de seguridad, Indicadores y Cuadro de Mando. Normas y Estándares. Las métricas permiten a los responsables de seguridad demostrar la eficiencia del programa de seguridad y el valor que aporta a la compañía. Documento en línea. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m292p.htm . Consulta: 22/02/2009.

Congreso de la República de Venezuela (1970). Ley de Universidades. Gaceta Oficial No. 1429, Extraordinario, del 8 de septiembre de 1970. Venezuela.

Gómez, D. y Quintero, M. (2008).Seguridad Informática. Servicio Nacional de Aprendizaje (SENA). Técnico Profesional en Administración del Talento Humano Recurso Humano. Documento en línea. Disponible en: <http://www.scribd.com/doc/6317119/Seguridad-a-Doc-Word1> . Consulta: 26/02/2009.

Molist, M. (1999). Aumentan los Ataques a Universidades y bajan en las Empresas, según las Estadísticas del CERT. Documento en línea. Disponible en: <http://ww2.grn.es/merce/1999/estadistiques.html> . Consulta: 15/03/2008.

Passarello, E. (2006). Convergencia de prácticas. Reflexiones y Tendencias. Consejo Profesional de Ingeniería en Electrónica, Telecomunicaciones y Computación (COPITEC). Documento en

línea. Disponible en: <http://www.scribd.com/doc/3796594/PASSARELLO-ESPEITO-Convergencia-de-Practicas> . Consulta: 30/03/2009.

Schneier, B. (2002). *Secrets and Lies. Digital Security in a Networked World*. EE.UU. John Wiley&Sons.

Universidad de Oriente (UNIVO) (2006). *Manual de Normas y Políticas de seguridad Informática*. Documento en línea. Disponible en: http://www.scribd.com/doc/2023909/manual-de-politicas-y-normas-de-seguridad-informatica#document_metadata. Consulta: 30/03/2009.

Vásquez, J. (2003). *¿Qué son las Organizaciones? Teoría y pensamiento administrativo*. Documento en línea. Disponible en: <http://www.gestiopolis.com/canales/gerencial/articulos/56/orgsqueson.htm> . Consulta: 30/04/2008.

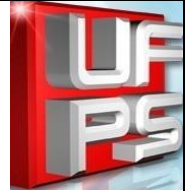
Villegas, M. (2008). *Modelo de Madurez para la Gestión y Administración de la Seguridad Informática en las Universidades*. Tesis de Maestría no publicada. Universidad Simón Bolívar, Venezuela.

ANEXOS

ANEXO A. ENTREVISTA N° 01



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
OCAÑA
ESPECIALIZACIÓN EN AUDITORIA EN SISTEMAS
INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE
BELÉN



ENTREVISTA N° 01

NOMBRE : __ _____
CARGO : __ _____
FECHA : _____
HORA INICIO: _____
HORA FIN: _____

Evalúe la seguridad informática en su empresa, dando respuestas a las preguntas del cuestionario:

Los ordenadores de su empresa, ¿tienen instalado antivirus?

El antivirus que tienen instalado (si es el caso), ¿está actualizado con las últimas definiciones?

¿Se realiza un mantenimiento informático periódico sobre los ordenadores de la empresa?

¿Se utilizan programas de descarga de archivos de usuario (música, películas, programas...)?

¿De cuántos ordenadores dispone su empresa?

¿Disponen de servidor central de datos en su empresa?

Sobre dicho servidor, ¿se realiza un mantenimiento informático periódico?



¿Dispone de baterías (SAI) para cada ordenador, para evitar apagones y sobretensiones?

¿Dispone de batería (SAI) para el servidor central, para evitar apagones y sobretensiones?

FIRMA
ENTREVISTADO

FIRMA
RESPONSABLE

ANEXO B. ENCUESTA N° 01

	<p align="center"> UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA ESPECIALIZACIÓN EN AUDITORIA EN SISTEMAS INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN </p>	
<p align="center">ENCUESTA N° 01</p> <p> NOMBRE :__ _____ CARGO : _____ FECHA : _____ HORA INICIO: _____ HORA FIN: _____ </p> <p><i>CONTROL DE OPERACIÓN</i></p> <ol style="list-style-type: none"> ¿Existen procedimientos formales para la operación del sistema de cómputo? SI () NO () ¿Están actualizados los procedimientos? SI () NO () Indique la periodicidad de la actualización de los procedimientos: Semestral () Anual () Cada vez que haya cambio de equipo () Indique el contenido de los instructivos de operación para cada aplicación: Identificación del sistema () Identificación del programa () Periodicidad y duración de la corrida () Especificación de formas especiales () Especificación de cintas de impresoras () Etiquetas de archivos de salida, nombre, () archivo lógico, y fechas de creación y expiración Instructivo sobre materiales de entrada y salida () Altos programados y la acciones requeridas () Instructivos específicos a los operadores en caso de falla del equipo () Instructivos de reinicio () Procedimientos de recuperación para proceso de gran duración o criterios () Identificación de todos los dispositivos de la máquina a ser usados () 		

- Especificaciones de resultados (cifras de control, registros de salida por archivo, etc.)
()
5. ¿Existen órdenes de proceso para cada corrida en la computadora (incluyendo pruebas, compilaciones y producción)?
SI () NO ()
 6. ¿Son suficientemente claras para los operadores estas órdenes?
SI () NO ()
 7. ¿Existe una estandarización de las ordenes de proceso?
SI () NO ()
 8. ¿Existe un control que asegure la justificación de los procesos en el computador? (Que los procesos que se están autorizados y tengan una razón de ser procesados.
SI () NO ()
 9. ¿Cómo programan los operadores los trabajos dentro del departamento de cómputo?
Primero que entra, primero que sale ()
se respetan las prioridades, ()
Otra (especifique) ()
 10. ¿Los retrasos o incumplimiento con el programa de operación diaria, se revisa y analiza?
SI () NO ()
 11. ¿Quién revisa este reporte en su caso?
 12. Analice la eficiencia con que se ejecutan los trabajos dentro del departamento de cómputo, tomando en cuenta equipo y operador, a través de inspección visual, y describa sus observaciones.
 13. ¿Existen procedimientos escritos para la recuperación del sistema en caso de falla?
 14. ¿Cómo se actúa en caso de errores?
 15. ¿Existen instrucciones específicas para cada proceso, con las indicaciones pertinentes?
 16. ¿Se tienen procedimientos específicos que indiquen al operador que hacer cuando un programa interrumpe su ejecución u otras dificultades en proceso?
 17. ¿Puede el operador modificar los datos de entrada?
 18. ¿Se prohíbe a analistas y programadores la operación del sistema que programo o analizo?
 19. ¿Se prohíbe al operador modificar información de archivos o bibliotecas de programas?
 20. ¿El operador realiza funciones de mantenimiento diario en dispositivos que así lo requieran?
 21. ¿Las intervenciones de los operadores: Son muy numerosas? SI () NO ()
¿Se limitan los mensajes esenciales? SI () NO ()
Otras (especifique) _____
 22. ¿Se tiene un control adecuado sobre los sistemas y programas que están en operación?
SI () NO ()
 23. ¿Cómo controlan los trabajos dentro del departamento de cómputo?
 23. ¿Se rota al personal de control de información con los operadores procurando un entrenamiento cruzado y evitando la manipulación fraudulenta de datos?
SI () NO ()
 24. ¿Cuentan los operadores con una bitácora para mantener registros de cualquier evento y

acción tomada por ellos?

Si ()

por máquina ()

escrita manualmente ()

NO ()



- 25.** Verificar que exista un registro de funcionamiento que muestre el tiempo de paros y mantenimiento o instalaciones de software.
- 26.** **27.** ¿Existen procedimientos para evitar las corridas de programas no autorizados?
SI () NO ()
- 27.** ¿Se permite a los operadores el acceso a los diagramas de flujo, programas fuente, etc. fuera del departamento de cómputo?
SI () NO ()
- 28.** ¿Se controla estrictamente el acceso a la documentación de programas o de aplicaciones rutinarias?
SI () NO ()
¿Cómo? _____
- 29.** Verifique que los privilegios del operador se restrinjan a aquellos que le son asignados a la clasificación de seguridad de operador.
- 30.** ¿Existen procedimientos formales que se deban observar antes de que sean aceptados en operación, sistemas nuevos o modificaciones a los mismos?
SI () NO ()
- 31.** ¿Estos procedimientos incluyen corridas en paralelo de los sistemas modificados con las versiones anteriores?
SI () NO ()
- 32.** ¿Durante cuánto tiempo?
- 33.** ¿Qué precauciones se toman durante el periodo de implantación?
- 34.** ¿Quién da la aprobación formal cuando las corridas de prueba de un sistema modificado o nuevo están acordes con los instructivos de operación.
- 35.** ¿Se catalogan los programas liberados para producción rutinaria?
SI () NO ()
- 36.** Mencione que instructivos se proporcionan a las personas que intervienen en la operación rutinaria de un sistema.
- 37.** Indique que tipo de controles tiene sobre los archivos magnéticos de los archivos de datos, que aseguren la utilización de los datos precisos en los procesos correspondientes.
- 38.** ¿Existe un lugar para archivar las bitácoras del sistema del equipo de cómputo?
SI () NO ()
- 39.** Indique como está organizado este archivo de bitácora.
- Por fecha ()
 - por fecha y hora ()
 - por turno de operación ()
 - Otros ()

40. ¿Cuál es la utilización sistemática de las bitácoras?
41. ¿Además de las mencionadas anteriormente, que otras funciones o áreas se encuentran en el departamento de cómputo actualmente?
42. Verifique que se lleve un registro de utilización del equipo diario, sistemas en línea y batch, de tal manera que se pueda medir la eficiencia del uso de equipo.
43. ¿Se tiene inventario actualizado de los equipos y terminales con su localización?
SI () NO ()
44. ¿Cómo se controlan los procesos en línea?
45. ¿Se tienen seguros sobre todos los equipos?
SI () NO ()
46. ¿Conque compañía?
Solicitar pólizas de seguros y verificar tipo de seguro y montos.
47. ¿Cómo se controlan las llaves de acceso (Password)?.

FIRMA
ENTREVISTADO

FIRMA
RESPONSABLE

ANEXO C. LISTA DE CHEQUEO N° 01

	<p align="center"> UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA ESPECIALIZACIÓN EN AUDITORIA EN SISTEMAS INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN </p>	
-----------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------

LISTA DE CHEQUEO N° 01

NOMBRE :__ _____
CARGO : __ _____
FECHA : _____
HORA INICIO: _____
HORA FIN: _____

Auditoría al Plan de Seguridad Informática

AUDITORÍA AL PLAN DE SEGURIDAD INFORMÁTICA				
ASPECTO A EVALUAR	SI	NO	NA	OBSERVACIONES
¿La Política de Seguridad de la Información (PSI) se encuentra formalmente establecida, aprobada y publicada?				
¿La PSI tiene una descripción y propósito?				
¿La PSI es conocida por todos los miembros de la empresa?				

<p>¿En la empresa se tiene establecido el Comité de Seguridad de la Información (CSI)?</p>				
<p>¿Se encuentra definido qué personal integra el CSI?</p>				
<p>¿Se ha designado a un Coordinador de Seguridad Informática?</p>				
<p>¿Realiza la Unidad de Auditoría Interna revisiones sobre la vigencia e implementación de la PSI?</p>				
<p>¿El Comité de Seguridad realiza al menos una capacitación anual sobre las PSI, tanto a colaboradores, docentes y estudiantes?</p>				
<p>¿Cuándo un empleado se retira, el Coordinador de Seguridad, elimina el usuario correspondiente a dicho empleado?</p>				
<p>¿Cuándo un empleado se retira, hace entrega del inventario de activos a su cargo?</p>				

<p>¿Se encuentran completamente identificados y clasificados los activos importantes asociados a cada sistema de información?</p>				
<p>¿Se elaboró un inventario con la información recabada sobre activos importantes?</p>				
<p>¿Se cuenta con informes de gestión que evalúen el accionar del Comité?</p>				
<p>¿Existen permisos de acceso para la información de acuerdo con las funciones y competencias?</p>				
<p>¿Se encuentra instalados antivirus en los servidores y estaciones de trabajo configurados para actualizaciones diarias?</p>				
<p>¿El Coordinador de Seguridad Informática monitorea permanentemente el tráfico de la red para detectar actividades inusuales o detrimento en el desempeño de la red?</p>				
<p>¿Existen copias de Seguridad de la información?</p>				

¿Se designó formalmente al responsable de la realización de las copias de seguridad?				
¿Se evidencia la presencia del registro de revisiones a las copias de seguridad?				
¿Existe un responsable de la custodia de las copias de seguridad?				
¿Las copias de seguridad se almacenan en un lugar externo a la empresa para prevenir pérdida de datos en el caso de una destrucción del centro de cómputo?				
¿Se encuentran las copias de seguridad y las claves de acceso debidamente protegidas ante casos de contingencia?				
¿Se cuenta con un servidor en paralelo, el cual permitirá la continuidad de las operaciones, en caso de falla del servidor principal?				
¿Se cuenta con mínimo un cortafuego (Firewall) que prevenga el acceso de intrusos al sistema?				
¿Se encuentra documentada la configuración de los enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red?				

¿Existen políticas y procedimientos para el desarrollo, adquisición y mantenimiento de software utilizado por la empresa?				
¿Cuenta el centro de cómputo con sistemas de control de acceso físico a sus instalaciones?				
¿Se investigan y monitorean los incidentes de seguridad?				
¿Cada aplicación instalada cuenta con la licencia?				
¿Las aplicaciones instaladas cuentan con rutinas de autorización de entrada?				
¿Se evidencia la presencia de los procedimientos de administración de cuentas de usuario para el uso de servicios de la red?				
¿Se evidencia la presencia de alertas de seguridad?				
¿Existe un documento donde se evidencie el cambio de contraseñas periódicas en las diferentes dependencias?				

¿Se encuentra restringido el acceso de páginas que no sean institucionales?				
¿El acceso a las aplicaciones está restringido a tres intentos máximo?				
¿Se encuentra restringido el acceso a los recursos de TI institucionales según los perfiles de usuario?				
¿El software adquirido en la empresa cuenta con mínimo certificación CMMI3?				
¿Las aplicaciones informáticas mantienen niveles de seguridad de acuerdo a los perfiles de usuario?				
¿Los programas fuente y las licencias se encuentran debidamente protegidas en sitios de máxima seguridad?				
¿Se evidencia la presencia del log de auditoría en las aplicaciones informáticas?				

<p>¿Se lleva una Bitácora con el control de cambios de las aplicaciones, indicando la fecha, hora, aplicación a la que se realizó el cambio, la causa, los cambios realizados y la persona que lo realizó?</p>				
<p>¿Se evidencia la presencia del documento de Registro de Incidencias de Seguridad Informática, donde quede consignado los datos de reporte del incidente y de la persona que reporta?</p>				
<p>¿El Coordinador de Seguridad Informática investiga las causas de los incidentes reportados y los registra en el documento de Registro de Incidencias de Seguridad Informática?</p>				
<p>¿Se evidencia la actualización de la Política de Seguridad Informática, mínimo cada año, en el documento Registro de Cambios de la Política de Seguridad Informática?</p>				
<p>¿Se evidencia la presencia del documento Plan de Continuidad del Negocio?</p>				

¿Las alternativas de mitigación tienen asignado personal responsable de ejecutarlas?				
<hr/> FIRMA ENTREVISTADO				<hr/> FIRMA RESPONSABLE

ANEXO D. OBSERVACIÓN DIRECTA

NOMBRE DEL TRABAJADOR: _____

CARGO : _____

FECHA : _____

SEGURIDAD FISICA

1. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información?
SI (X) NO ()
2. ¿Existen una persona responsable de la seguridad?
SI (X) NO ()
3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?
SI (X) NO () DOS CELADORES .
4. ¿Existe personal de vigilancia en la institución?
SI (X) NO ()
5. ¿La vigilancia se contrata?
a) Directamente ()
b) Por medio de empresas que venden ese servicio (X)
6. ¿Existe una clara definición de funciones entre los puestos clave?
SI (X) NO ()
6. ¿Se investiga a los vigilantes cuando son contratados directamente?
SI (X) NO ()
7. ¿Se controla el trabajo fuera de horario?
SI () NO (X)
8. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?.
SI () NO (X)
9. ¿Existe vigilancia en el departamento de cómputo las 24 horas?
SI () NO (X)
10. ¿Existe vigilancia a la entrada del departamento de cómputo las 24 horas?
a) Vigilante ? ()
b) Recepcionista? ()
c) Tarjeta de control de acceso ? ()
d) Nadie? (X)
11. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?
SI () NO (X)

12. Se ha instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?
SI () NO (X)
13. El edificio donde se encuentra la computadora está situado a salvo de:
a) Inundación? ()
b) Terremoto? ()
c) Fuego? ()
d) Sabotaje? ()
14. El centro de cómputo tiene salida al exterior al exterior?
SI (X) NO ()
15. ¿Existe control en el acceso a este cuarto?
a) Por identificación personal? ()
b) Por tarjeta magnética? ()
c) por claves verbales? ()
d) Otras? (X) NO SE REALIZA
16. ¿Son controladas las visitas y demostraciones en el centro de cómputo?
SI () NO (X)
17. ¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática?
SI () NO (X)
18. ¿Se vigilan la moral y comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar un posible fraude?
SI () NO (X)
19. ¿Existe alarma para
a) Detectar fuego(calor o humo) en forma automática? ()
b) Avisar en forma manual la presencia del fuego? ()
c) Detectar una fuga de agua? ()
d) Detectar magnéticos? ()
e) No existe (X)
20. ¿Estas alarmas están
a) En el departamento de cómputo? ()
b) En la cintoteca y discoteca? ()
21. ¿Existe alarma para detectar condiciones anormales del ambiente?
a) En el departamento de cómputo? ()
b) En la cínoteca y discoteca? ()
c) En otros lados ()
24. ¿La alarma es perfectamente audible?
SI () NO (X)
20. 25.¿Esta alarma también está conectada
a) Al puesto de guardias? ()
b) A la estación de Bomberos? ()
c) A ningún otro lado? (X)
Otro_____

22. Existen extintores de fuego
a) Manuales? ()
b) Automáticos? ()
c) No existen (X)
23. ¿Se ha adiestrado el personal en el manejo de los extintores?
SI () NO (X)
24. ¿Los extintores, manuales o automáticos a base de TIPO SI NO
a) Agua, () (X)
b) Gas? () (X)
c) Otros () (X)
25. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?
SI () NO (X)
26. ¿Si es que existen extintores automáticos son activador por detectores automáticos de fuego?
SI () NO (X)
27. ¿Si los extintores automáticos son a base de agua ¿Se han tomado medidas para evitar que el agua cause más daño que el fuego?
SI () NO (X)
28. ¿Si los extintores automáticos son a base de gas, ¿Se ha tomado medidas para evitar que el gas cause más daño que el fuego?
SI () NO (X)
29. ¿Existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos para que el personal
a) Corte la acción de los extintores por tratarse de falsas alarmas? SI () NO (X)
b) Pueda cortar la energía Eléctrica SI () NO (X)
c) Pueda abandonar el local sin peligro de intoxicación SI () NO (X)
d) Es inmediata su acción? SI () NO ()
30. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?
SI () NO (X)
31. ¿Saben que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?
SI () NO (X)
32. ¿El personal ajeno a operación sabe qué hacer en el caso de una emergencia (incendio)?
SI () NO (X)
33. ¿Existe salida de emergencia?
SI (X) NO ()
34. ¿Esta puerta solo es posible abrirla:
a) Desde el interior ? ()
b) Desde el exterior ? ()
c) Ambos Lados (X)

35. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?
SI (X) NO ()
36. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?
SI () NO (X)
37. ¿Se ha tomado medidas para minimizar la posibilidad de fuego:
a) Evitando artículos inflamables en el departamento de cómputo? ()
b) Prohibiendo fumar a los operadores en el interior? ()
c) Vigilando y manteniendo el sistema eléctrico? ()
d) No se ha previsto ()
38. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?
SI () NO ()
39. ¿Se limpia con frecuencia el polvo acumulado debajo del piso falso si existe?
SI () NO () NO EXISTE
40. ¿Se controla el acceso y préstamo en la
a) Discoteca? ()
b) Cintoteca? ()
c) Programoteca? ()
41. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?
SI (X) NO ()
42. Explique la forma en que están protegidas físicamente estas copias (bóveda, cajas de seguridad etc.) que garantice su integridad en caso de incendio, inundación, terremotos, etc.
NO ESTAN PROTEGIDAS, ESTAN EN CD
43. ¿Se tienen establecidos procedimientos de actualización a estas copias?
SI (X) NO ()
44. Indique el número de copias que se mantienen, de acuerdo con la forma en que se clasifique la información:
0 1 2 3
45. ¿Existe departamento de auditoría interna en la institución?
SI () NO (X)
46. ¿Este departamento de auditoría interna conoce todos los aspectos de los sistemas?
SI () NO (X)
47. ¿Cuándo se efectúan modificaciones a los programas, a iniciativa de quién es?
a) Usuario ()
b) Director de informática ()
c) Jefe de análisis y programación ()
d) Programador ()
e) Otras (especifique) __RECTOR__
48. ¿La solicitud de modificaciones a los programas se hacen en forma?
a) Oral? (X)

- b) Escrita? ()
En caso de ser escrita solicite formatos,
49. Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?
SI (X) NO ()
50. ¿Existe control estricto en las modificaciones?
SI () NO (X)
51. ¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?
SI () NO (X)
52. ¿Si se tienen terminales conectadas, ¿se ha establecido procedimientos de operación?
SI () NO (X)
53. Se verifica identificación:
a) De la terminal ()
b) Del Usuario ()
c) No se pide identificación ()
63. ¿Se ha establecido que información puede ser acezada y por qué persona?
SI (X) NO ()
54. ¿Se ha establecido un número máximo de violaciones en sucesión para que la computadora cierre esa terminal y se de aviso al responsable de ella?
SI () NO (X) NO HAY LIMITE DE INTENTOS
55. ¿Se registra cada violación a los procedimientos con el fin de llevar estadísticas y frenar las tendencias mayores?
SI () NO (X)

ANEXO E. DICTAMEN



Cúcuta, 29 de Agosto de 2013

Señor:

Carlos Luis Villamizar

Rector Institución Educativa Nuestra Señora de Belén

Presente:

Debido a la falta de una guía de auditoría en la Institución Educativa Nuestra Señora de Belén el rector del establecimiento educativo, solicitó a la Empresa **KBL AUDITORES** se realizara una auditoria en el área de secretaria dado que el flujo de la información que se maneja es mayor; la cual se realiza mediante uso de la plataforma web Webcolegios, que le permite el manejo de la información de los docentes, alumnos, notas, etc. Con la realización de la auditoria, se pretende evaluar la seguridad de la información tanto física como lógica del área secretaria.

La auditoría fue evaluada en la seguridad lógica y física de sistemas de información empleados en el área de secretaria del Establecimiento Educativo Nuestra Señora de Belén de la ciudad de Cúcuta, en la parte de infraestructura, el diseño y niveles de seguridad.

Terminada la auditoría se observó que el área de secretaria, carece de políticas de seguridad, por lo cual se recomienda la creación de unas políticas de seguridad de manera que se minimicen los riesgos que se pueden presentar y se realicen los controles necesarios ya sean preventivos o correctivos de las situaciones presentadas.

Ing. LeidyYoana Bayona
Auditora Líder

Clasificación del Documento: Publico	INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN	Pág.98De 13
-----------------------------------------	-----------------------------------------------------	-------------

HISTORIAL DE REVISIONES

REV._	ELABORADO	REVISADO	APROBADO
NOMBRE	Leidy Y Bayona		
CARGO	Jefe del Grupo		
FIRMA			
FEHCA	01-Junio-2013		

Clasificación del Documento: Publico	INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN	Pág.99De 13
<p style="text-align: center;">Resolución No. ____</p> <p>Por la cual se regulan las políticas de seguridad informática y el uso adecuado de la tecnología para el procesamiento de la información en la Institución Educativa Nuestra Señora de Belén</p> <p style="text-align: center;">EL RECTOR DE LA INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN En uso de sus facultades legales y estatutarias y CONSIDERANDO</p> <ul style="list-style-type: none"> ✓ Que la Institución Educativa Nuestra Señora de Belén, reconoce que la información es un activo valioso y que se requieren políticas adecuadas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la misma. ✓ Que la Constitución Política en su Artículo 61 establece que el Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley. ✓ Que la Institución Educativa Nuestra Señora de Belén debe promover y proteger la producción intelectual de los miembros de su comunidad mediante el reconocimiento debido de los derechos morales y patrimoniales generados. <p>ALCANCE.</p> <p>Las políticas de seguridad, definidas el presente documento, aplican a todos los funcionarios públicos y contratistas de la Institución Educativa Nuestra Señora de Belén, y otras personas vinculadas que utilicen los recursos informáticos de la Institución.</p> <p>También describe todas las normas, políticas y estándares que se aplicarán de manera obligatoria de parte del personal con respecto a seguridad informática para precautelar un correcto uso de equipos de cómputo y aplicaciones tecnológicas; para el presente manual se ha considerado sugerencias y recomendaciones del estándar británico británicas BS7799.</p> <p>BS7799 hace énfasis en la integridad, confidencialidad y disponibilidad. Integridad se refiere a la necesidad de proteger la exactitud de la información, así como los métodos utilizados para procesarla. Confidencial se refiere a la garantía de que la información sólo puede ser visitada por las personas que tienen la autorización para hacerlo. Y la disponibilidad se refiere a la garantía de que aquellos que han sido autorizadas a hacer uso de la información tienen acceso a ella y todos los asociados activos cuando sea necesario.</p> <p>En este manual, se describen cinco secciones, que representan la seguridad en varios campos de acción de los usuarios, las cuales son:</p> <ul style="list-style-type: none"> ✓ SEGURIDAD PERSONAL ✓ SEGURIDAD FÍSICA Y AMBIENTAL ✓ SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO 		

Clasificación del Documento: Publico	INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN	Pág.100De 13
<p>✓ CONTROL DE ACCESO LÓGICO ✓ CUMPLIMIENTO</p> <p>Cada capítulo incluye la política relacionada, así como el conjunto de normas respectivas consideradas en cada caso.</p> <p>CARACTERIZACIÓN DEL SISTEMA INFORMÁTICO.</p> <p>La Institución Educativa Colegio Nuestra Señora de Belén, cuenta con una serie de recursos tecnológicos de carácter institucional y administrativo, que incorporan labores del talento humano que trabaja ahí, por tal motivo es fundamental reconocer los riesgos que implica el uso de esas herramientas y las condiciones ideales que optimizan su productividad, para tales fines es fundamental el desarrollo de políticas de seguridad que apoyen estos procesos y que apunten a un modelo sostenible, productivo, progresivo y adaptable a los ritmos acelerados de la tecnología.</p> <p>Como se mencionó anteriormente, dentro de los recursos tecnológicos de la Institución Educativa Colegio Nuestra Señora de Belén cuenta:</p> <ul style="list-style-type: none"> ✓ Con bienes informáticos, tales como una sala de informática y computadores para educar para uso institucional. ✓ No cuenta con una red que comunique todas las estaciones de trabajo dentro de la institución, pero utilizan una plataforma contratada por el centro educativo, para el manejo de notas del alumno por internet, que es manejado por varios usuarios, tales como el estudiante, el padre o acudiente, y funcionarios del establecimiento que manejan la plataforma Webcolegios. <p>PROPÓSITO:</p> <p>Se hace necesario el establecimiento de las políticas de seguridad informáticas que protejan, preserven y administren correctamente la información de la universidad, junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.</p> <p>Que en mérito de lo expuesto,</p> <p>Que todos los funcionarios públicos y contratistas vinculados con la INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELEN deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades.</p>		

Clasificación del Documento: Publico	INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN	Pág.101De 13
<p>Que el otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin.</p> <p>Que todas las prerrogativas para el uso de los sistemas de información de la Entidad deben terminar inmediatamente después de que el trabajador cesare de prestar sus servicios a la Entidad.</p> <p>Que los proveedores o terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas.</p> <p>Que por lo anteriormente expuesto,</p> <p>RESUELVE:</p> <p>ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN</p> <p>El Comité de Seguridad de la información de la Universidad estará integrado por:</p> <ul style="list-style-type: none"> ✓ Un Coordinador de Seguridad de la Información, el cual deberá acreditar estudios y/o experiencia en Seguridad Informática o en Auditoría de Sistemas. ✓ El Director del Departamento de Sistemas. ✓ Jefe de la oficina de Talento Humano o un delegado especializado. <p>Los integrantes del Comité velarán por el cumplimiento de los siguientes objetivos de seguridad:</p> <ul style="list-style-type: none"> • Revisar y proponer al Rector, para su consideración y posterior aprobación, las políticas de seguridad de la información y las funciones generales en materia de seguridad de la información que fuera convenientes y apropiadas. <p>2) Monitorear cambios significativos en los riesgos que afectan a los recursos de la información frente a posibles amenazas, sean internas o externas.</p> <p>3) Evaluar y coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios de la Institución, sean preexistente o nuevos.</p> <p>4) Promover la difusión y cumplimiento de las Políticas de Seguridad establecidas.</p> <p>5) Coordinar a las diferentes dependencias en materia de seguridad de la información.</p> <p>6) Aprobar y revisar anualmente el Plan de Continuidad.</p>		

Clasificación del Documento: Publico	INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN	Pág.102De 13
<p>7) Aprobar el Plan Anual de Auditorías a realizar.</p> <p>DESCRIPCIÓN DE LAS POLITICAS</p> <p>POLITICA0:INFORMACIÓN Y DATOS INSTITUCIONALES U OFICIALES Es toda aquella información y datos que se utilizan en todos los Procesos y Procedimientos del Sistema Integrado de Gestión para el logro de los objetivos, metas, propósitos misionales y la satisfacción al cliente y que se maneja, transfiere y procesa en un medio tal como: papel, auditivos, visuales, digitales, electrónicos y/o cualquier otro medio que las circunstancias propias de la gestión y/o de los avances tecnológicos se requieran para el cumplimiento de las obligaciones y responsabilidades legales de la Institución.</p> <p>Cualquier otro tipo de información que no esté contemplada en la Política 0, no será Institucional u Oficial y en consecuencia no está permitido su uso, manipulación, transferencia, procesamiento a través de los Recursos de Informáticos y/o cualquier otro mecanismo o medio de manejo.</p> <p>POLITICA1:ACCESO A LA INFORMACIÓN</p> <p>Todos los funcionarios públicos, contratistas, y pasantes que laboran para la Institución deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación.</p> <p>El otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin.</p> <p>Todas las prerrogativas para el uso de los sistemas de información de la Institución deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la Entidad Proveedores o terceras personas solamente deben tener privilegios durante el periodo Del tiempo requerido para llevar a cabo las funciones aprobadas.</p> <p>Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la ajena sala Institución, la rectoría, la Secretaria General, los jefes de procesos deben autorizar Entidad, la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal de la Entidad.</p> <p>Para acceder a la plataforma Webcolegios los usuarios deberán hacerlo a través de su plena identificación y utilizando la contraseña correspondiente. La cuenta de correo institucional es de</p>		

Clasificación del Documento: Publico	INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN	Pág.103De 13
<p>uso exclusivo para las actividades relacionadas con sus funciones o con la prestación del servicio.</p> <p>La cuenta de correo está formada por el nombre del usuario y contraseña, es privada e intransferible, siendo responsabilidad de proteger la clave de acceso o password, no debe prestar la clave bajo ninguna circunstancia, pues su uso recae bajo su responsabilidad del usuario.</p> <p>El proceso de autenticación debe ser de máximo tres intentos para una autenticación satisfactoria, después de éste número de intentos la cuenta será bloqueada.</p> <p>Las contraseñas deben tener una vigencia de noventa días, una vez vence dicho plazo su cambio deberá ser obligatorio.</p> <p>Únicamente usuarios administrativos están autorizados para utilizar software que permita descifrar las contraseñas y comprobar que se está cumpliendo con las políticas establecidas al respecto.</p> <p>Deberán comunicar a rectoría o persona encargada, el Sistema Nacional de Talento Humano la relación de funcionarios públicos que hayan ingresado a laborar y de los que han dejado de hacerlo, para la activación o desactivación de las cuentas de correo respectivas, así mismo la Oficina Asesora Jurídica y de Contratación enviará la relación del personal vinculado mediante contratos y de los que han terminado el plazo de ejecución.</p> <ol style="list-style-type: none"> 1. Inicio y terminación de las sesiones del sistema operativo 2. Intentos de crear, remover, definir contraseñas o modificar los privilegios del sistema operativo 3. Modificaciones en la configuración de las estaciones 4. Accesos (login) y de salidas (logoff) del sistema operativo 5. Intentos de acceso no autorizado al sistema operativo <p>POLITICA2:ADMINISTRACION DE CAMBIOS</p> <p>Todo cambio (creación y modificación de programas, pantallas y reportes) que afecte los recursos informáticos, debe ser requerido por los usuarios de la información y aprobado formalmente por el responsable de la administración del mismo, al nivel de jefe inmediato o a quien es estos formalmente deleguen. El responsable de la administración de los accesos tendrá la facultad de aceptar o rechazarla solicitud.</p> <p>POLITICA3:SEGURIDADDE LA INFORMACIÓN</p> <p>Los funcionarios públicos, contratistas, y pasantes de la Institución son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Entidad, por la Ley para proteger la y evitar pérdidas, accesos no autorizados, exposición y</p>		

Clasificación del Documento: Publico	INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN	Pág.104De 13
<p>utilización indebida de la misma.</p> <p>Los funcionarios públicos, contratistas, y pasantes no deben suministrar cualquier información de la entidad a ningún ente externo sin las autorizaciones respectivas.</p> <p>Todo funcionario que utilice los Recursos Informáticos, tiene la responsabilidad de Velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por eservalegal o ha sido clasificada como confidencial y/o crítica.</p> <p>Los funcionarios, contratistas y pasantes deben firmar y renovar cada año, un acuerdo de cumplimiento de la seguridad de la información, la confidencialidad y el buen manejo de la información. Después de que el trabajador deja de prestar sus servicios a la Entidad, se compromete entregar toda la información respectiva de su trabajo realizado. Una vez retirado el funcionario, contratista o pasante de la Institución Educativa Nuestra Señora de Belén deben comprometerse a no utilizar, comercializar o divulgar los productos o a información generada o conocida durante la gestión en la entidad, directamente o través de terceros, así mismo, los funcionarios públicos que detecten el mal uso de la información está en la obligación de reportar el hecho a la oficina de control interno.</p> <p>Contar con roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles. También deben permitir que un rol de usuario administre el Administrador de usuarios.</p> <p>Las puertas traseras: Las puertas traseras son entradas no convencionales a los sistemas operacionales, bases de datos y aplicativos. Es de suma importancia aceptarla existencia de las mismas en la mayoría de los sistemas operacionales, bases de datos, aplicativos y efectuar las tareas necesarias para contrarrestar la vulnerabilidad que ellas generan.</p> <p>El control de acceso a todos los sistemas de computación de la entidad debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario.</p> <p>Las palabras claves o contraseñas de acceso a los recursos informáticos, quede sign en los funcionarios públicos, contratistas y pasantes de la Institución son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.</p> <p>Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales</p>		

Clasificación del Documento: Publico	INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN	Pág.105De 13
--------------------------------------	--------------------------------------------------	--------------

El Usuario es el único responsables por el cuidado y buen uso de los recursos informáticos entregados para realizar sus actividades laborales.

Creación de un plan de mantenimiento de equipos.

Verificar que el software de antivirus esté actualizado y habilitado, en caso de recibir alguna advertencia del software antivirus o sospecha que su antivirus no ha sido actualizado, debe avisar inmediatamente para dar soporte a la plataforma y realizar las respectivas copias de seguridad.

POLITICA6:SEGURIDADEN COMUNICACIONES

Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, deberán ser consideradas y tratadas como información confidencial.

Características del procesamiento, transmisión y conservación de la información, teniendo en cuenta el flujo interno y externo y los niveles de clasificación de la misma.

POLÍTICA7:SEGURIDADPARAUSUARIOS TERCEROS

Los dueños de los Recursos Informáticos que no sean propiedad de la entidad y deban ser ubicados y administrados por ésta, deben garantizar la legalidad del recurso para su funcionamiento. Adicionalmente debe definir un documento de acuerdo oficial entre las partes.

Cuando se requiera utilizar recursos informáticos o otros elementos de propiedad de Institución para el funcionamiento de recursos que no sean propios de la entidad y que deban ubicarse en sus instalaciones, los recursos serán administrados por el área técnica de la Institución o docente encargado informar al coordinador.

Los usuarios terceros tendrán acceso a los Recursos Informáticos, que sean estrictamente necesarios para el cumplimiento de su función, servicios que deben ser probados por quien será el Jefe inmediato o coordinador.

POLÍTICA8:SOFTWARE UTILIZADO

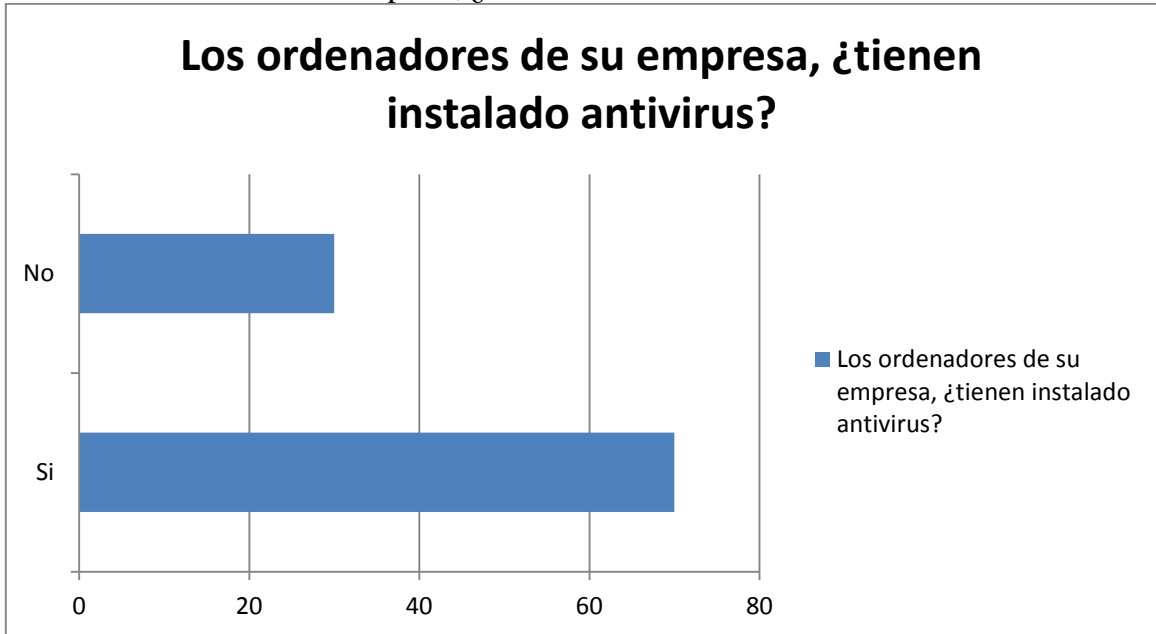
Existirá un inventario de las licencias de software de la Institución que permita su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado. Todo software que utilice la Institución será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Entidad o reglamentos internos.

Clasificación del Documento: Publico	INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN	Pág.106De 13
<p>Todo el software de manejo de datos que utilice la Institución dentro de su infraestructura informática, deberá contar con las técnicas más avanzadas de la industria para garantizar la integridad de los datos.</p> <p>Instalar únicamente aplicaciones autorizadas y concernientes a las actividades laborales y de servicios.</p> <p>Está prohibido exportar software o información técnica o copia no autorizada de material protegido por derechos de autor que incluye, pero no está limitado a, digitalización y distribución de imágenes o fotografías de cualquier origen, digitalización y distribución de música, audio o video, distribución o instalación de software sin licencia ni autorización de la Institución.</p> <p>Debe existir una cultura informática al interior de la Entidad que garantice el conocimiento por parte de los funcionarios públicos, contratistas y pasantes de las implicaciones que tiene el instalar software ilegal en los computadores de la Institución.</p> <p>POLÍTICA9:ACTUALIZACION DE HARDWARE</p> <p>Cualquier cambio que se requiera realizaren los equipos de cómputo de la entidad (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del área responsable.</p> <p>La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado.</p> <p>Los equipos de microcomputadores (PC, servidores, LAN etc.)No deben moverse o reubicarse sin la aprobación previa del administrador, jefe o coordinador del área involucrada.</p> <p>Actualización periódica del inventario tecnológico.</p> <p>Gestión de compras: Requisición, Proveedores, órdenes y control de devoluciones Cualquier equipo que requiera salir o ser trasladado a otro lugar debe solicitarse con previa autorización e informarse al respectivo coordinador o jefe inmediato.</p> <p>POLÍTICA10:ALMACENAMIENTOY RESPALDO</p> <p>La información que es soportada por la infraestructura de tecnología informática de la Institución deberá ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad.</p>		

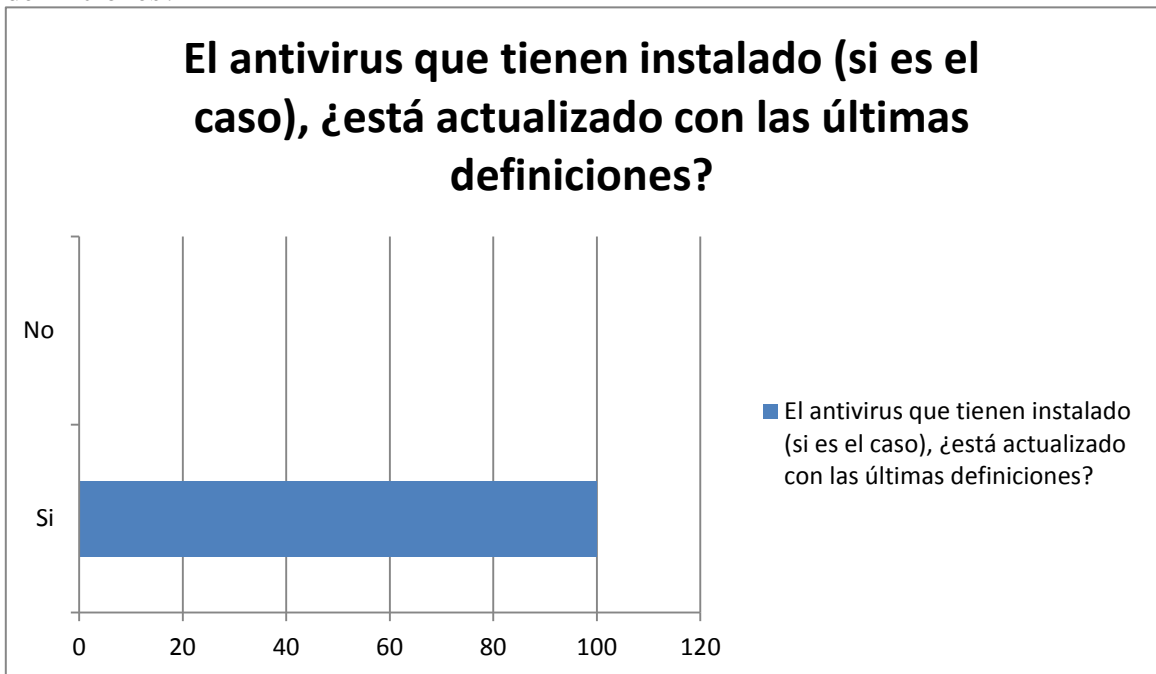
Clasificación del Documento: Publico	INSTITUCIÓN EDUCATIVA NUESTRA SEÑORA DE BELÉN	Pág.107De 13
<p>Debe existir una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo.</p> <p>La entidad definirá la custodia de los respaldos de la información que se realizará externamente con una compañía especializada en este tema.</p> <p>El almacenamiento de la información deberá realizarse interna y/o externamente a la Entidad, esto de acuerdo con la importancia de la información para la operación de la Institución.</p> <p>POLITICA11:CONTINGENCIA</p> <p>La administración de la Institución debe preparar, actualizar periódicamente y probar en forma regular un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes desproporciones como terremoto, explosión, terrorismo, inundación etc.</p> <p>Debe contar con copias de seguridad en diferentes lugares con acceso restringido en caso de que cualquier eventualidad se presente y requiera su uso, la información esté disponible.</p> <p>POLÍTICA12:ESCRITORIOS LIMPIOS</p> <p>Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD, USB, u otro dispositivo de almacenamiento, con fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante el horario normal de trabajo y fuera del mismo.</p> <p>POLÍTICA13:ADMINISTRACION DE LA SEGURIDAD</p> <p>La evaluación de riesgos de seguridad para los Recursos Informáticos se debe ejecutar al menos una vez cada año. Todas las mejoras, actualizaciones, conversiones y cambios relativos asociados con estos recursos deben ser precedidos por una evaluación.</p> <p>Se deben evaluar los inconvenientes que se han presentado para detectar las fallas y si se requiere capacitar al personal que maneja dicha información para que el incidente no vuelva a ocurrir.</p> <p>El plan de políticas de la información debe ser conocido por todo el personal vinculado que maneje información de la Institución y en cuyo caso se hace relevante que en su totalidad sea comunicado.</p>		

ANEXO G. RESULTADOS DE LA ENTREVISTA N° 01

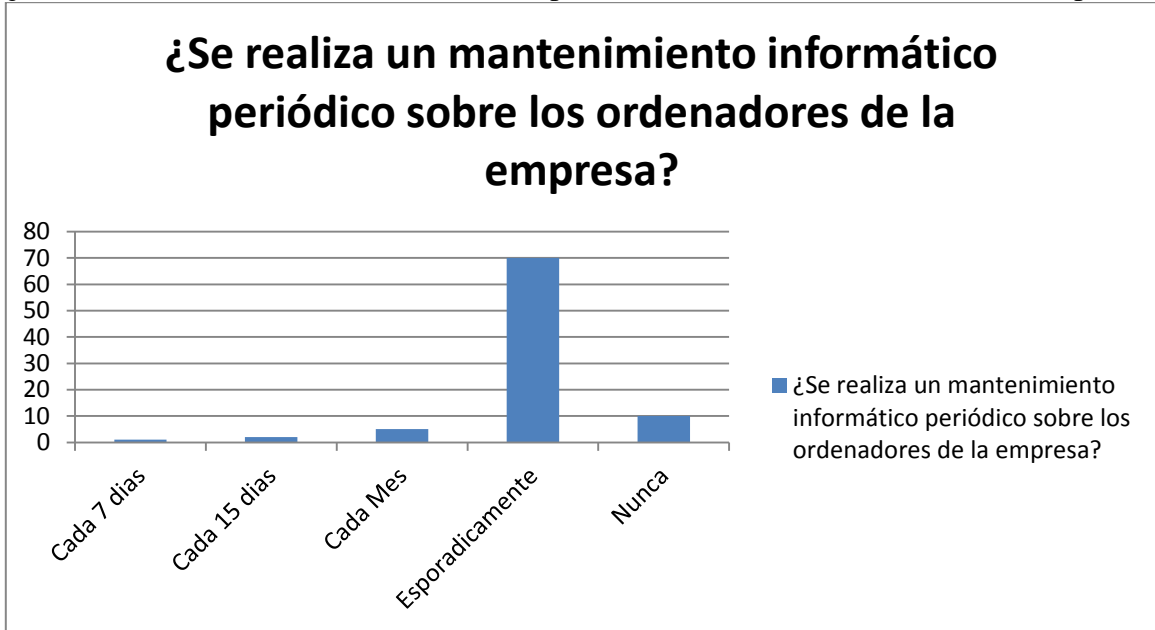
1. Los ordenadores de su empresa, ¿tienen instalado antivirus?



2. El antivirus que tienen instalado (si es el caso), ¿está actualizado con las últimas definiciones?



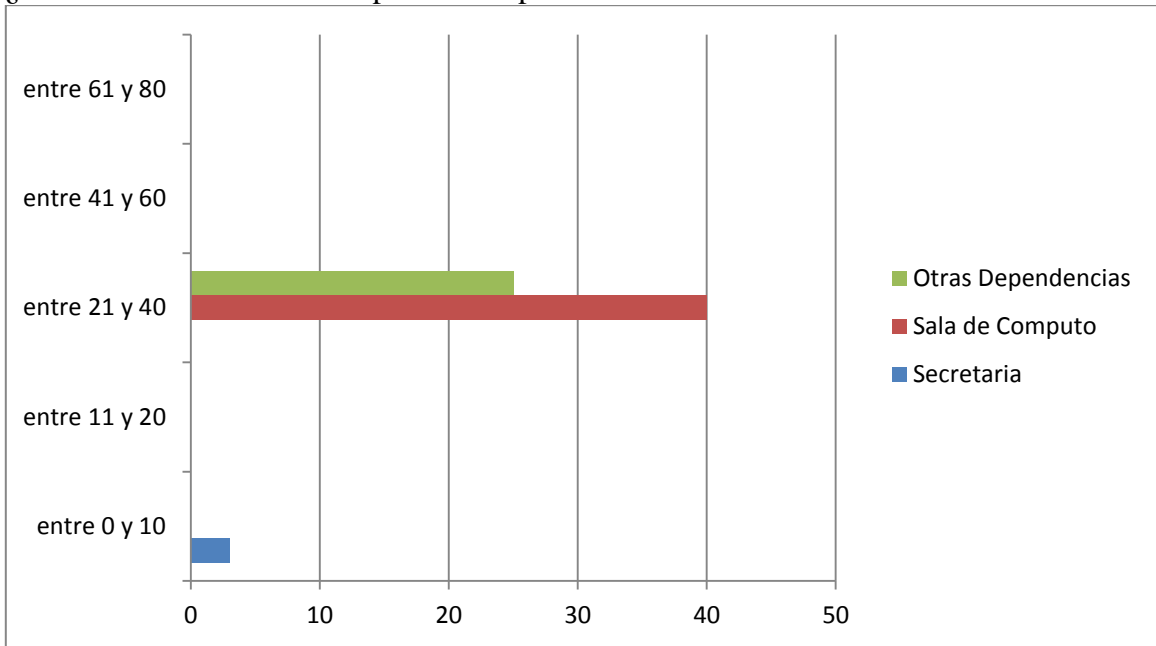
3. ¿Se realiza un mantenimiento informático periódico sobre los ordenadores de la empresa?



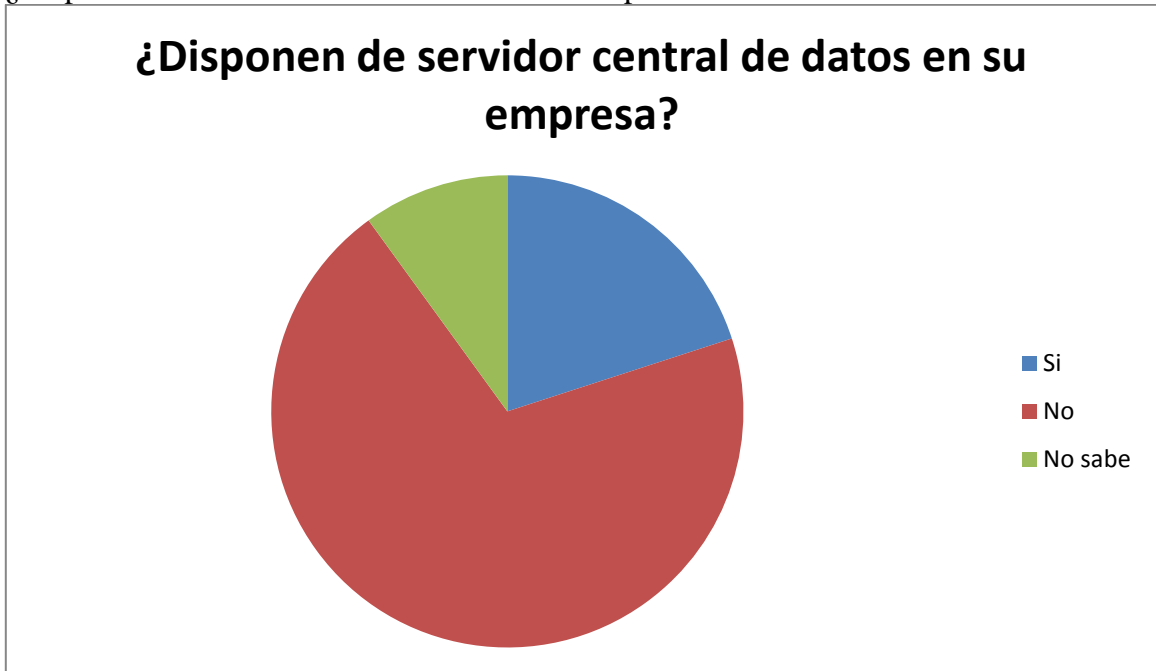
4. ¿Se utilizan programas de descarga de archivos de usuario (música, películas, programas...)?



5. ¿De cuántos ordenadores dispone su empresa?



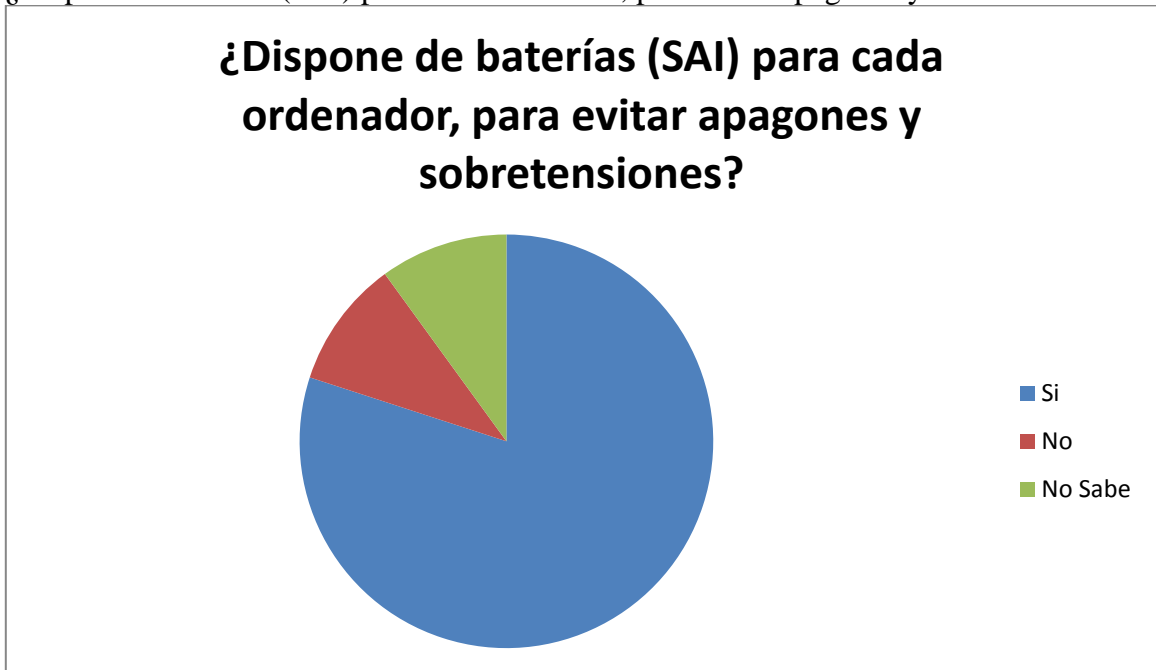
6. ¿Disponen de servidor central de datos en su empresa?



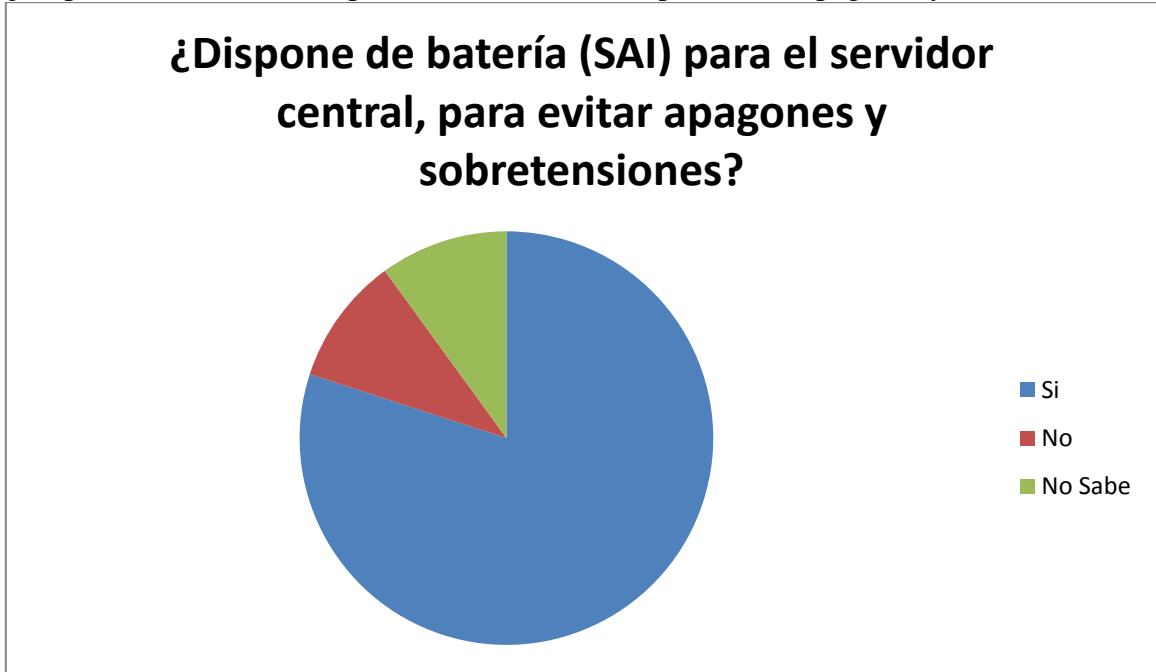
7. Sobre dicho servidor, ¿se realiza un mantenimiento informático periódico?



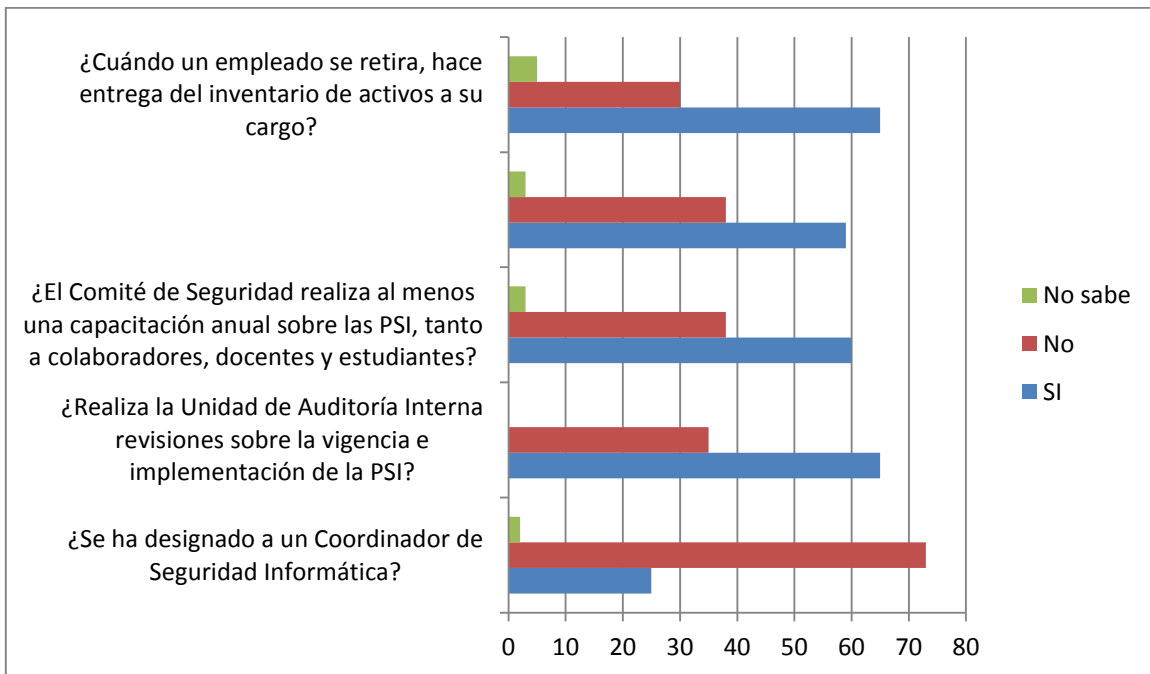
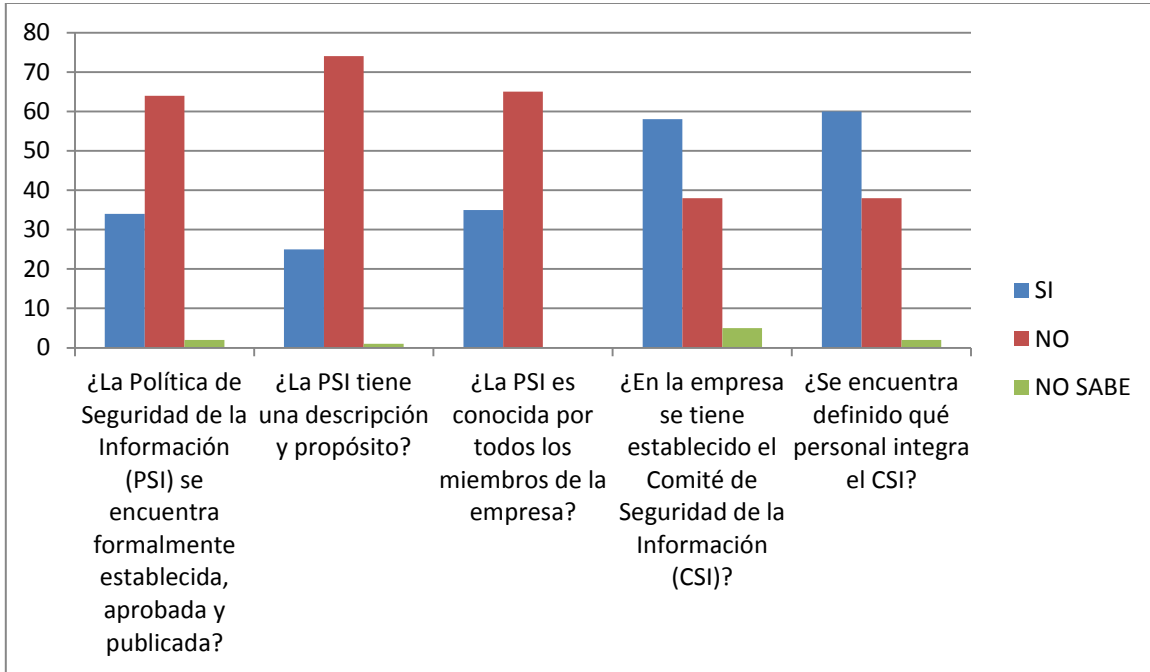
8. ¿Dispone de baterías (SAI) para cada ordenador, para evitar apagones y sobretensiones?

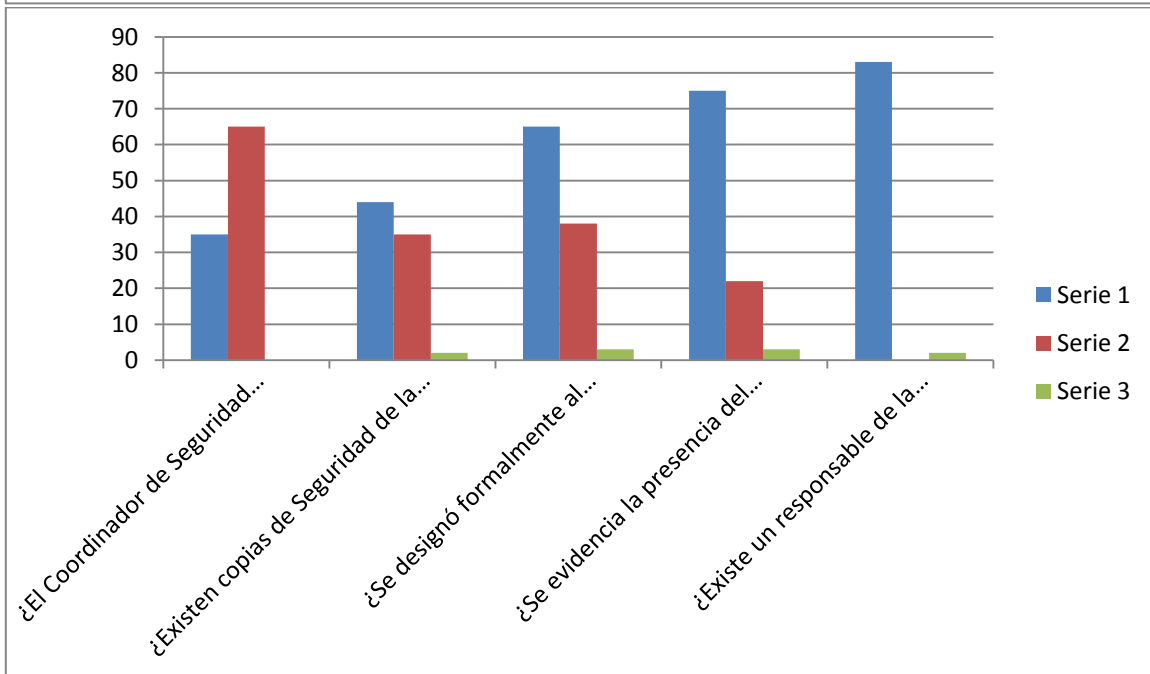
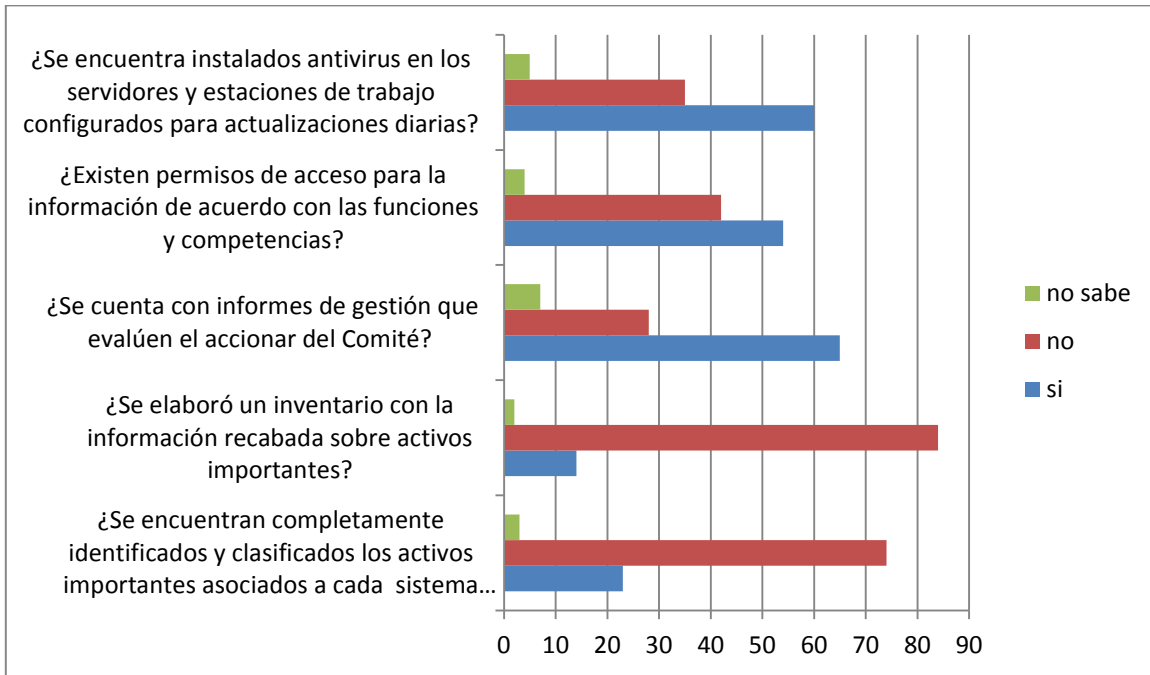


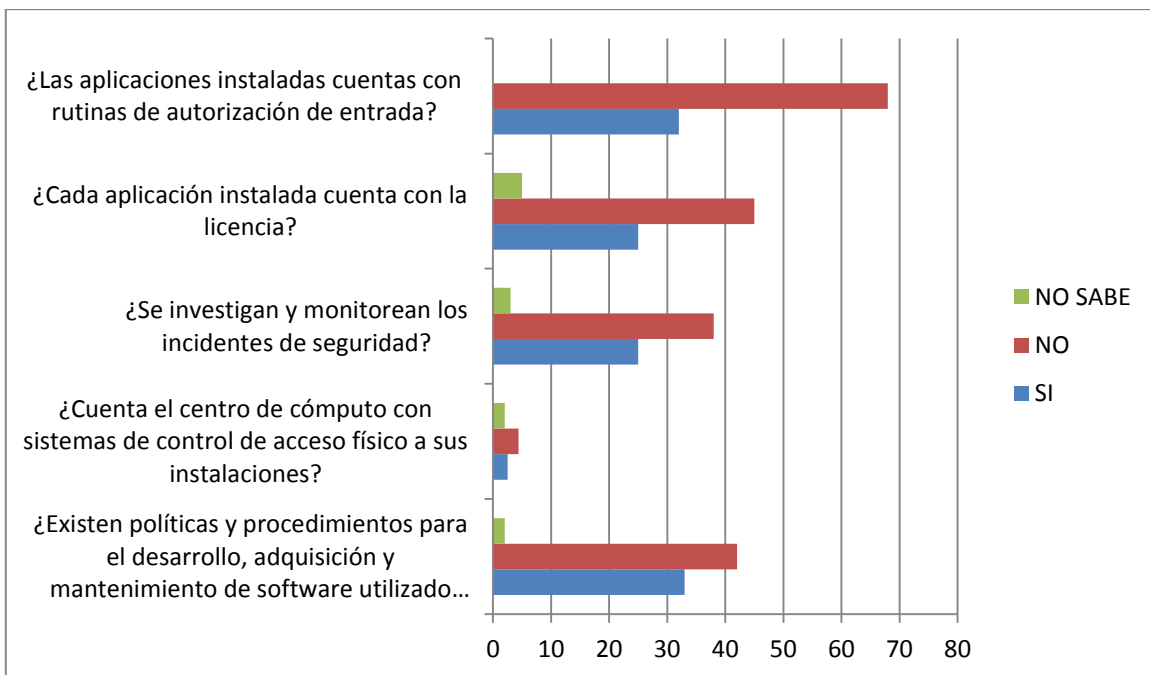
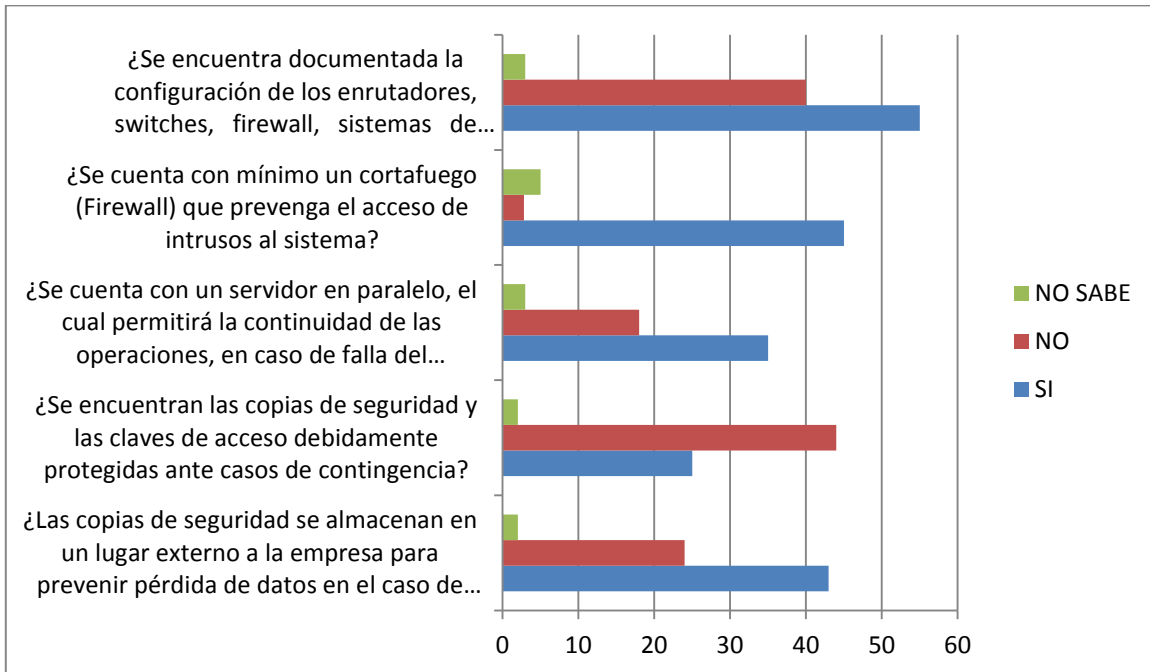
9. ¿Dispone de batería (SAI) para el servidor central, para evitar apagones y sobretensiones?

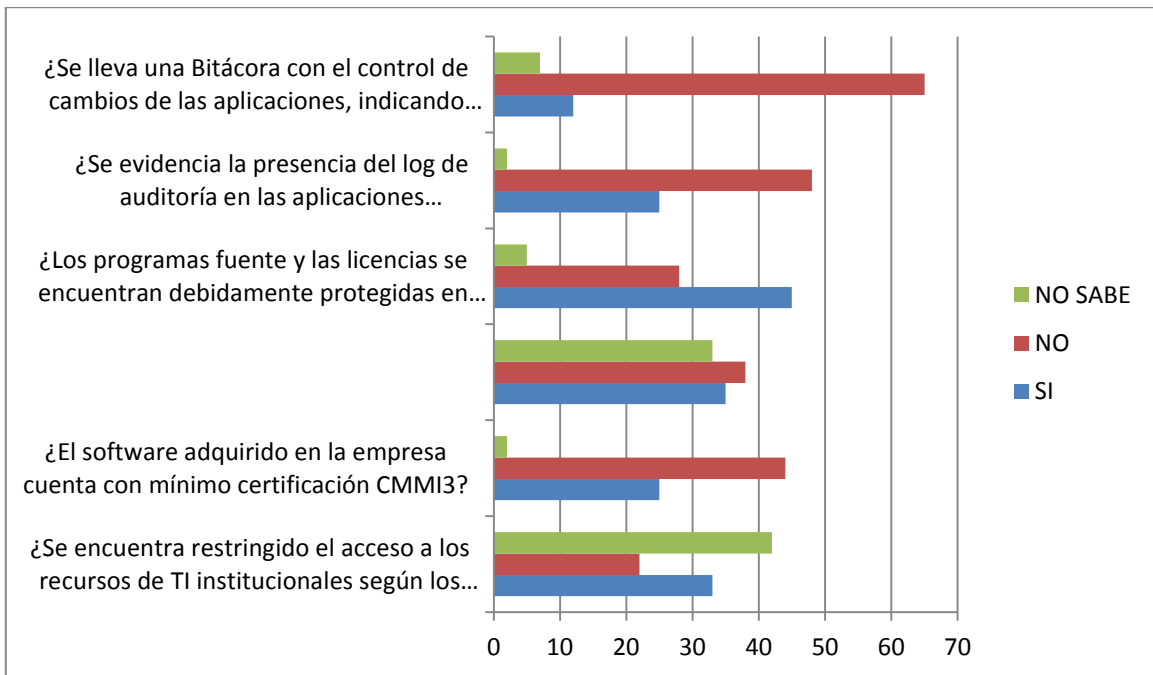
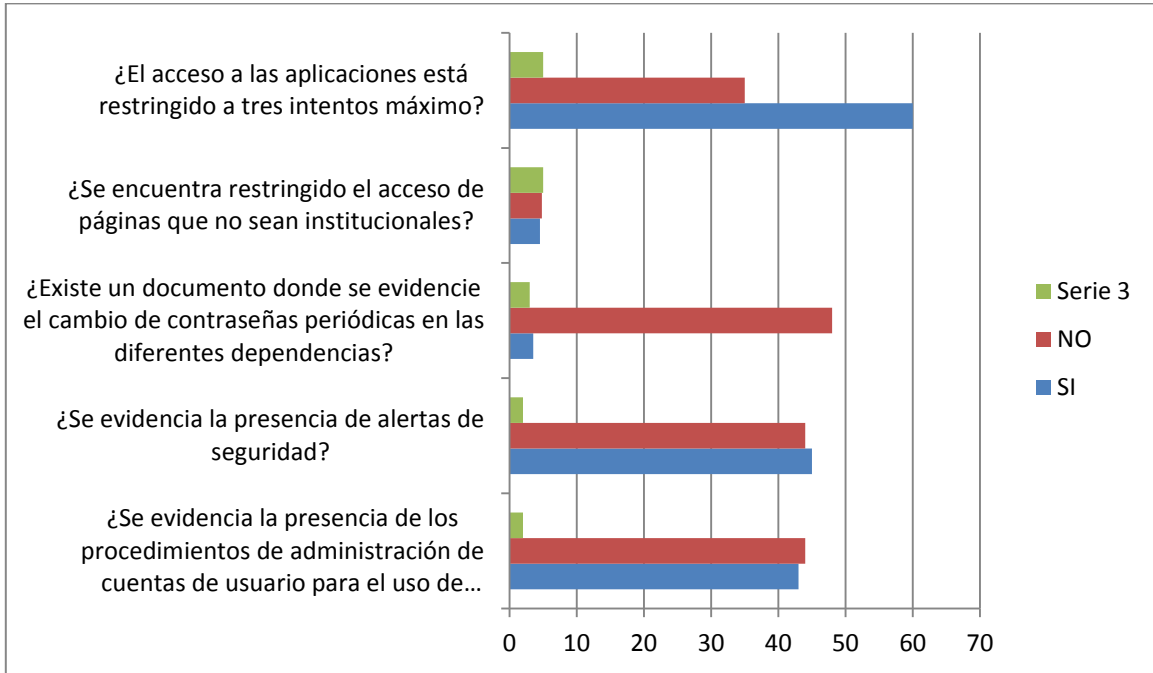


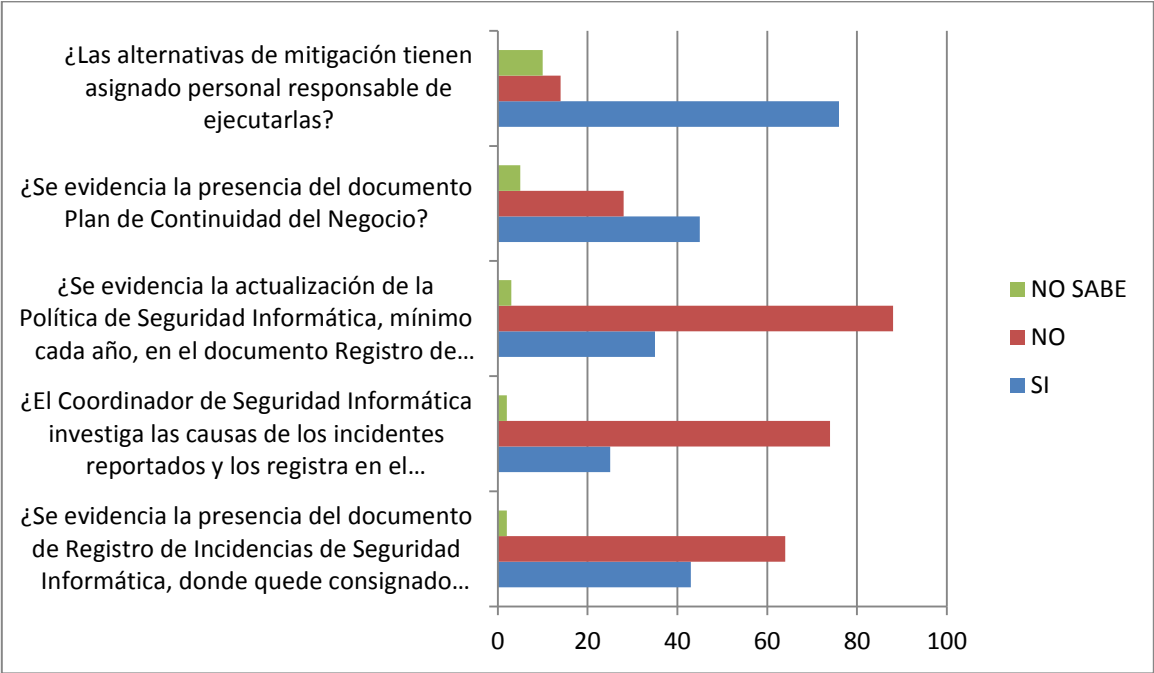
ANEXO H. RESULTADOS DE LISTA DE CHEQUEO











ANEXO I RESULTADOS DE OBSERVACION DIRECTA

SEGURIDAD FISICA

16. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información?
SI (X) NO ()
17. ¿Existen una persona responsable de la seguridad?
SI (X) NO ()
18. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?
SI (X) NO () DOS CELADORES .
19. ¿Existe personal de vigilancia en la institución?
SI (X) NO ()
20. ¿La vigilancia se contrata?
 - a) Directamente ()
 - b) Por medio de empresas que venden ese servicio (X)
6. ¿Existe una clara definición de funciones entre los puestos clave?
SI (X) NO ()
21. ¿Se investiga a los vigilantes cuando son contratados directamente?
SI (X) NO ()
22. ¿Se controla el trabajo fuera de horario?
SI () NO (X)
23. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?.
SI () NO (X)
24. ¿Existe vigilancia en el departamento de cómputo las 24 horas?
SI () NO (X)
25. ¿Existe vigilancia a la entrada del departamento de cómputo las 24 horas?
 - a) Vigilante ? ()
 - b) Recepcionista? ()
 - c) Tarjeta de control de acceso ? ()
 - d) Nadie? (X)
26. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?
SI () NO (X)
27. Se ha instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?
SI () NO (X)
28. El edificio donde se encuentra la computadora está situado a salvo de:
 - a) Inundación? ()
 - b) Terremoto? ()

- c) Fuego? ()
d) Sabotaje? ()
29. El centro de cómputo tiene salida al exterior al exterior?
SI (X) NO ()
30. ¿Existe control en el acceso a este cuarto?
a) Por identificación personal? ()
b) Por tarjeta magnética? ()
c) por claves verbales? ()
d) Otras? (X) NO SE REALIZA
21. ¿Son controladas las visitas y demostraciones en el centro de cómputo?
SI () NO (X)
22. ¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática?
SI () NO (X)
23. ¿Se vigilan la moral y comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar un posible fraude?
SI () NO (X)
24. ¿Existe alarma para
a) Detectar fuego(calor o humo) en forma automática? ()
b) Avisar en forma manual la presencia del fuego? ()
c) Detectar una fuga de agua? ()
d) Detectar magnéticos? ()
e) No existe (X)
56. ¿Estas alarmas están
a) En el departamento de cómputo? ()
b) En la cintoteca y discoteca? ()
57. ¿Existe alarma para detectar condiciones anormales del ambiente?
a) En el departamento de cómputo? ()
b) En la cínoteca y discoteca? ()
c) En otros lados ()
24. ¿La alarma es perfectamente audible?
SI () NO (X)
25. 25.¿Esta alarma también está conectada
a) Al puesto de guardias? ()
b) A la estación de Bomberos? ()
c) A ningún otro lado? (X)
Otro _____
58. Existen extintores de fuego
a) Manuales? ()
b) Automáticos? ()
c) No existen (X)
59. ¿Se ha adiestrado el personal en el manejo de los extintores?
SI () NO (X)

60. ¿Los extintores, manuales o automáticos a base de TIPO SI NO
a) Agua, () (X)
b) Gas? () (X)
c) Otros () (X)
61. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?
SI () NO (X)
62. ¿Si es que existen extintores automáticos son activador por detectores automáticos de fuego?
SI () NO (X)
63. ¿Si los extintores automáticos son a base de agua ¿Se han tomado medidas para evitar que el agua cause más daño que el fuego?
SI () NO (X)
64. ¿Si los extintores automáticos son a base de gas, ¿Se ha tomado medidas para evitar que el gas cause más daño que el fuego?
SI () NO (X)
65. ¿Existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos para que el personal
a) Corte la acción de los extintores por tratarse de falsas alarmas? SI () NO (X)
b) Pueda cortar la energía Eléctrica SI () NO (X)
c) Pueda abandonar el local sin peligro de intoxicación SI () NO (X)
d) Es inmediata su acción? SI () NO ()
66. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?
SI () NO (X)
67. ¿Saben que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?
SI () NO (X)
68. ¿El personal ajeno a operación sabe qué hacer en el caso de una emergencia (incendio)?
SI () NO (X)
69. ¿Existe salida de emergencia?
SI (X) NO ()
70. ¿Esta puerta solo es posible abrirla:
a) Desde el interior ? ()
b) Desde el exterior ? ()
c) Ambos Lados (X)
71. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?
SI (X) NO ()
72. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?
SI () NO (X)

73. ¿Se ha tomado medidas para minimizar la posibilidad de fuego:
 a) Evitando artículos inflamables en el departamento de cómputo? ()
 b) Prohibiendo fumar a los operadores en el interior? ()
 c) Vigilando y manteniendo el sistema eléctrico? ()
 d) No se ha previsto ()
74. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?
 SI () NO ()
75. ¿Se limpia con frecuencia el polvo acumulado debajo del piso falso si existe?
 SI () NO () NO EXISTE
76. ¿Se controla el acceso y préstamo en la
 a) Discoteca? ()
 b) Cintoteca? ()
 c) Programoteca? ()
77. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?
 SI (X) NO ()
78. Explique la forma en que están protegidas físicamente estas copias (bóveda, cajas de seguridad etc.) que garantice su integridad en caso de incendio, inundación, terremotos, etc.
 NO ESTAN PROTEGIDAS, ESTAN EN CD
79. ¿Se tienen establecidos procedimientos de actualización a estas copias?
 SI (X) NO ()
80. Indique el número de copias que se mantienen, de acuerdo con la forma en que se clasifique la información:
 0 1 2 3
81. ¿Existe departamento de auditoría interna en la institución?
 SI () NO (X)
82. ¿Este departamento de auditoría interna conoce todos los aspectos de los sistemas?
 SI () NO (X)
83. ¿Cuándo se efectúan modificaciones a los programas, a iniciativa de quién es?
 a) Usuario ()
 b) Director de informática ()
 c) Jefe de análisis y programación ()
 d) Programador ()
 e) Otras (especifique) RECTOR
84. ¿La solicitud de modificaciones a los programas se hacen en forma?
 a) Oral? (X)
 b) Escrita? ()
 En caso de ser escrita solicite formatos,
85. Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?
 SI (X) NO ()
86. ¿Existe control estricto en las modificaciones?
 SI () NO (X)

87. ¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?
SI () NO (X)
88. ¿Si se tienen terminales conectadas, ¿se ha establecido procedimientos de operación?
SI () NO (X)
89. Se verifica identificación:
a) De la terminal ()
b) Del Usuario ()
c) No se pide identificación ()
63. ¿Se ha establecido que información puede ser acezada y por qué persona?
SI (X) NO ()
90. ¿Se ha establecido un número máximo de violaciones en sucesión para que la computadora cierre esa terminal y se de aviso al responsable de ella?
SI () NO (X) NO HAY LIMITE DE INTENTOS
91. ¿Se registra cada violación a los procedimientos con el fin de llevar estadísticas y frenar las tendencias mayores?
SI () NO (X)