UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
ESCUELA DE CONTABILIDAD SUPERIOR

TÍTULO: "AUDITORÍA DE SEGURIDAD INFORMÁTICA AL SISTEMA CONTABLE DE LA UNIDAD EDUCATIVA LA ASUNCIÓN, PARA EL PERÍODO 2017."

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN CONTABILIDAD Y AUDITORÍA

AUTORA: Denisse Gabriela Uyaguari Chalco

DIRECTOR: Ing. Pablo Fernando Pintado Zumba

CUENCA – ECUADOR

2017

DECLARACIÓN

Yo, Denisse Gabriela Uyaguari Chalco, declaro por honor y asumo la originalidad del presente trabajo de titulación, siendo de exclusiva responsabilidad de la autora, y que no he utilizado fuentes sin citarlas debidamente.

Denisse Gabriela Uyaguari Chalco

AGRADECIMIENTOS

En primer lugar, quiero agradecer a Dios por bendecirme durante el tiempo de estudio y poder culminar esta etapa universitaria. También, agradezco a la Unidad Educativa “La Asunción” por permitirme realizar el desarrollo de este trabajo de titulación.

A mi director de tesis, Ing. Pablo Pintado por su dirección y apoyo durante la elaboración de este trabajo.

Finalmente, a mis padres por el apoyo y comprensión incondicional que me han brindado en mis estudios, motivándome continuamente en mi formación profesional.

DEDICATORIA

A Dios

Quien me ilumina y me da sabiduría para poder alcanzar mis logros y metas propuestas.

A mis padres Gabriel y Olga

Por sus sacrificios, apoyo y comprensión absoluta que han contribuido en la formación de mi vida profesional.

A mi hermana Jessica

Por su apoyo en mis estudios y elaboración de este trabajo de titulación.

ÍNDICE DE CONTENIDO

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

RESUMEN

El presente trabajo de titulación: “Auditoría de seguridad informática al sistema contable de la Unidad Educativa La Asunción, para el período 2017”, investiga el ambiente relacionado con la seguridad informática del sistema contable en la unidad educativa, estudio que permitirá ejecutar la auditoría analizando el cumplimiento de las buenas prácticas de gestión de seguridad de la información basado en la norma ISO 27002. Finalmente, se da a conocer mediante el informe los hallazgos encontrados, conclusiones y recomendaciones pertinentes.

ABSTRACT

This graduation work entitled: "*Auditoria de seguridad informática al sistema contable de la Unidad Educativa La Asunción, para el período 2017*", examined the computer security environment of the accounting system in the educational institution. This study will allow the execution of the audit by analyzing compliance with good information security management practices based on the ISO 27002 standard. Finally, findings, conclusions and recommendations were informed through the report.

UNIVERSIDAD DEL AZUAY
Dpto. Idiomas

Translated by,
Lic. Lourdes Crespo

INTRODUCCIÓN

Hoy en día muchas entidades públicas o privadas no cuentan con el asesoramiento adecuado sobre la seguridad informática al sistema contable; lo que conlleva un alto riesgo de vulnerabilidad de pérdida o alteración de información crítica y por ende un impacto alto en el accionar diario de las entidades.

La auditoría informática, es fundamental dentro de las entidades ya que permite detectar vulnerabilidades y/o debilidades en la gestión informática y de seguridad de la información, proveyendo recomendaciones para fortalecer los pilares de la seguridad de la información como lo son la disponibilidad, confidencialidad e integridad de la información, con controles adecuados para evitar incidentes, fraudes o eventualidades.

En conclusión, se ha decidido llevar a cabo la auditoría informática al sistema contable de la Unidad Educativa La Asunción, basada en la norma ISO 27002 – Controles de Seguridad que recomienda abordar objetivos de control derivados de los riesgos para la confidencialidad, integridad y disponibilidad de información. Considerando que este trabajo de investigación ayudará a mejorar la gestión y desarrollo de buenas prácticas de seguridad de la información.

CAPÍTULO I

Fundamentos generales

1.1 Introducción

Este capítulo tiene como finalidad, dar a conocer una descripción general de la Unidad Educativa y del departamento financiero-contable a ser auditado mediante su historia, misión, visión, organigrama orgánico y funcional, y la situación actual de la seguridad informática del sistema contable.

1.2 Historia

En octubre de 1963, la comunidad de madres de la Asunción funda la escuela y colegio en la ciudad de Cuenca. Posteriormente, el 5 de octubre de 1973 se transformó en colegio Fiscomisional, implementándose el sistema de educación personalizada. Después de 10 años, se convierte en un colegio experimental y en el año de 1988, se modifica como Unidad Educativa mixta. En el año 2000, se inicia la implementación del Sistema de Gestión de Calidad 9001:2000. Consecutivamente, se obtiene la Certificación en el año 2006. Actualmente, La Unidad Educativa La Asunción es un centro educativo que tiene 54 años de vida constitucional adscrito a la Universidad del Azuay.

1.3 Misión

De acuerdo al Proyecto Educativo Institucional 2012-2018 la misión de la Unidad Educativa La Asunción es la siguiente:

"Somos una Unidad Educativa Particular en mejora continua, conformada por profesionales en constante actualización, que brinda a niños y jóvenes un servicio educativo humanístico–integral, acorde con las últimas tendencias pedagógicas,

científicas y tecnológicas, en un ambiente de calidez, compromiso y responsabilidad social.” (Unidad Educativa La Asuncion, 2017)

1.4 Visión

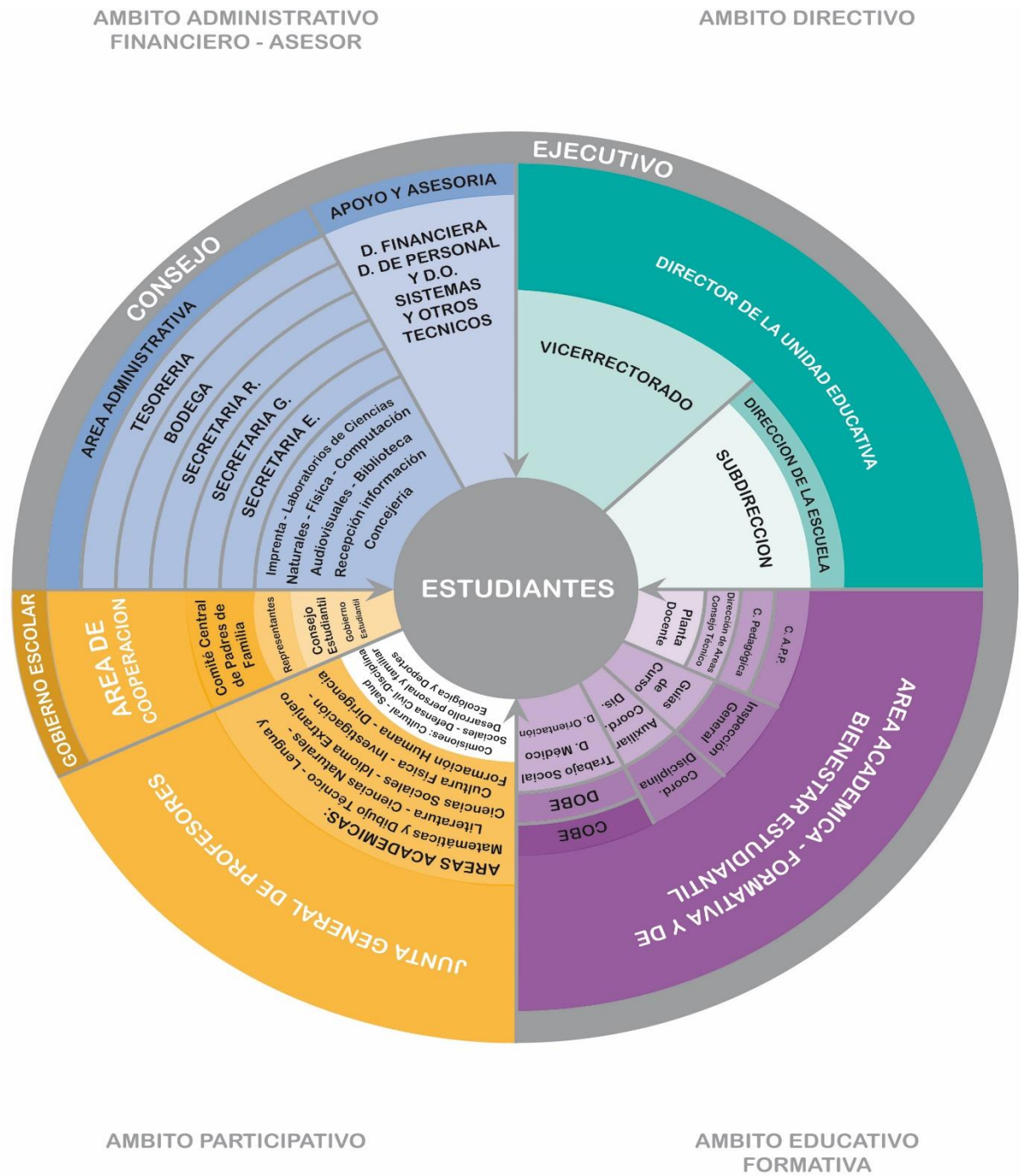
De acuerdo al Proyecto Educativo Institucional 2012-2018 la visión de la Unidad Educativa La Asunción es la siguiente:

“Consolidarnos como Unidad Educativa de confianza y reconocimiento social, que se mantenga a la vanguardia de la educación, con propuestas pedagógicas innovadoras, ofreciendo una formación de seres humanos íntegros, que contribuyan a su transformación personal y del entorno social y ambiental.” (Unidad Educativa La Asunción , 2017)

1.5 Estructura orgánico general

Actualmente, la Unidad Educativa dispone del siguiente organigrama general:

Ilustración 1 Estructura organizacional de la Unidad Educativa La Asunción



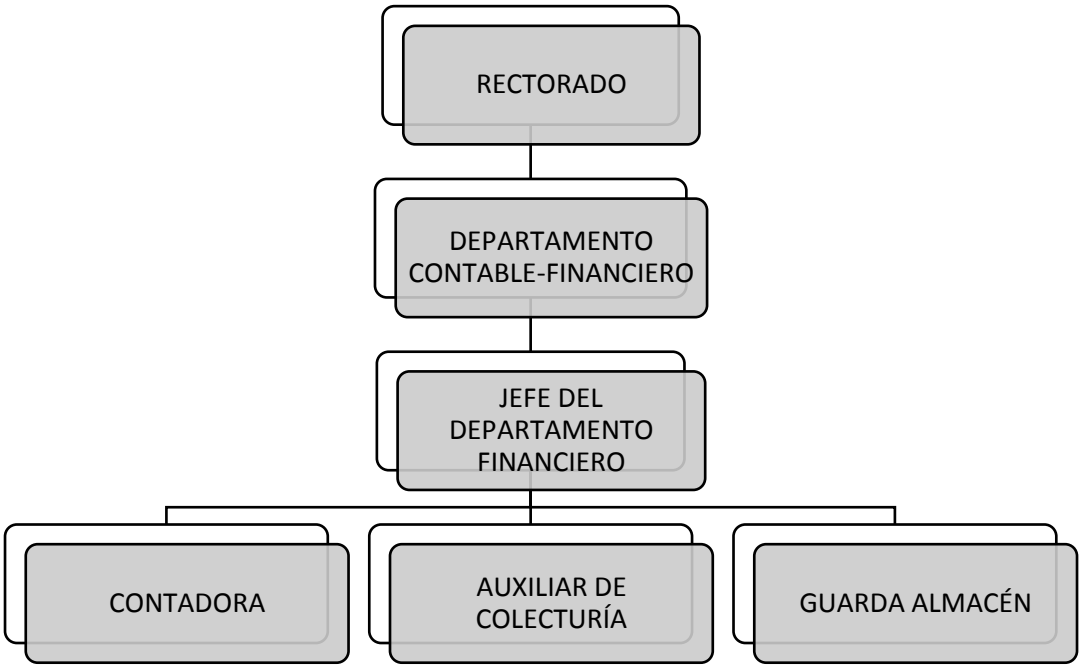
Realizado por: Master. José Zhunio. – Proyecto Educativo institucional (José, 2012)

1.6 Estructura orgánico-funcional del departamento Contable-Financiero y Sistemas

1.6.1 Estructura orgánica

Ilustración 2 Estructura organizacional - Departamento contable - financiero

DEPARTAMENTO CONTABLE- FINANCIERO



Realizado por: La autora

Ilustración 3 Estructura Organizacional - Departamento de Sistemas

DEPARTAMENTO DE SISTEMAS

Realizado por: La autora

1.6.2 Estructura funcional

La Unidad Educativa no presenta un organigrama funcional oficialmente establecido en el departamento contable-financiero y sistemas, debido a la reestructuración que se está realizando por cambio de las autoridades.

1.7 Situación actual de la seguridad informática del sistema contable en la unidad educativa La Asunción

Actualmente, la seguridad informática del sistema contable de la Unidad Educativa se encuentra dividido en dos partes. Principalmente, su dirección, control, mantenimiento y respaldo interno está a cargo del Tecnólogo José Galarza, Jefe del Departamento de Sistemas.

Por otra parte, el programa que se maneja en el departamento Contable-Financiero se encuentra tercerizado, es decir, se trabaja con una empresa externa denominada MENTREL SOFT desde el año 2008 a cargo del Ing. Ali Mendez, quien brinda mantenimiento, respaldo y soporte de forma administrativa, financiera y contable. El sistema tiene diferentes módulos como bancos, compras, ventas e inventarios, que permiten emitir facturas digitalizadas y se están actualizando constantemente de acuerdo a los requisitos exigidos por el Ministerio de Educación y el Servicio de Rentas Internas.

El acceso al programa SINET es otorgado por la empresa tercerizadora, mediante usuarios y claves de ingreso de acuerdo a las funciones y actividades que se necesiten desempeñar. En el presente, lo tienen las 4 personas que se encuentran laborando en el departamento contable-financiero.

Los respaldos que se realizan de la base de datos del programa, son realizados por el proveedor de tres a cuatro veces por mes y en la unidad educativa son respaldados por la contadora en el disco duro.

Al trabajar con programadores externos, se ha presentado como principal inconveniente la demora en ser solucionados los problemas causados o creación de reportes nuevos en el sistema contable, debido a que se tiene que esperar la presencia de la empresa tercerizadora. Otra falencia que se ha presentado en el programa del sistema contable,

es que no presenta avisos de alertas en caso de que las codificaciones de las cuentas contables se estén registrando incorrectamente, generando descuadres que se tiene que estar revisando constantemente. En los meses que se realiza las matrículas, se necesita que el proveedor ejecute la programación y conexiones en varios servidores para agilitar el proceso, el mismo que funciona únicamente con disponibilidad de red.

CAPÍTULO II

Buenas prácticas de seguridad de la información.

2.1 Reseña histórica de la Norma ISO 17799

La BSI por sus siglas en inglés definida como British Normal Institution, es una empresa multinacional que tiene como objetivo principal la creación de normas de estandarización de calidad y las publica bajo el prefijo “BS”.

La ISO 17799 proviene de la norma BS 7799 que hace referencia a la seguridad del “e-commerce.com” entre los compradores y vendedores. Esta norma se divide en dos partes, la primera parte se conoce como “Código de Prácticas”, y la segunda parte se define como “Especificaciones del sistema de administración de seguridad de la Información”.

En el año 2000, la primera parte de esta norma se formalizó y fue publicada como ISO 17799 considerada como una guía de recomendaciones de la seguridad de la información, su estructura se basa en 10 dominios de control: políticas de seguridad, aspectos organizativos para la seguridad, clasificación y control de activos, seguridad ligada al personal, seguridad física y del entorno, gestión de comunicaciones y operaciones, control de accesos, desarrollo y mantenimiento de sistemas, gestión de continuidad del negocio y conformidad con la legislación; ofreciendo todos ellos ventajas organizacionales. Mientras que el año 2002, la segunda parte de esta norma fue analizada y armonizada con otras normas ISO.

La norma ISO 17799 pasa a ser la ISO 27001 en el año 2005, después de 2 años se renombra como ISO 27002:2005. Finalmente, en el año 2013 esta norma tiene su última actualización.

2.2 Generalidades de la Norma ISO 27002 – Controles de Seguridad

La Norma ISO 27002 es una guía de buenas prácticas de seguridad de la información, cuyo objetivo principal es planificar, hacer, comprobar y mejorar mediante 14 dominios, 35 objetivos generales y 114 controles que expone dicha norma, brindando soluciones y recomendaciones de gestión de seguridad de la información en base a todos los riesgos que se expone la organización diariamente.

Ilustración 4 ISO/IEC 27002:2013

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

- 5. **POLÍTICAS DE SEGURIDAD.**
  - 5.1 Directrices de la Dirección en seguridad de la información.
    - 5.1.1 Conjunto de políticas para la seguridad de la información.
    - 5.1.2 Revisión de las políticas para la seguridad de la información.
- 6. **ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.**
  - 6.1 Organización interna.
    - 6.1.1 Asignación de responsabilidades para la segur. de la información.
    - 6.1.2 Segregación de tareas.
    - 6.1.3 Contacto con las autoridades.
    - 6.1.4 Contacto con grupos de interés especial.
    - 6.1.5 Seguridad de la información en la gestión de proyectos.
  - 6.2 Dispositivos para movilidad y teletrabajo.
    - 6.2.1 Política de uso de dispositivos para movilidad.
    - 6.2.2 Teletrabajo.
- 7. **SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.**
  - 7.1 Antes de la contratación.
    - 7.1.1 Investigación de antecedentes.
    - 7.1.2 Términos y condiciones de contratación.
  - 7.2 Durante la contratación.
    - 7.2.1 Responsabilidades de gestión.
    - 7.2.2 Concienciación, educación y capacitación en seguridad. de la información.
    - 7.2.3 Proceso disciplinario.
  - 7.3 Cese o cambio de puesto de trabajo.
    - 7.3.1 Cese o cambio de puesto de trabajo.
- 8. **GESTIÓN DE ACTIVOS.**
  - 8.1 Responsabilidad sobre los activos.
    - 8.1.1 Inventario de activos.
    - 8.1.2 Propiedad de los activos.
    - 8.1.3 Uso aceptable de los activos.
    - 8.1.4 Devolución de activos.

13.1.3 Segregación de redes.

13.2 Intercambio de información con partes externas.

13.2.1 Políticas y procedimientos de intercambio de información.

13.2.2 Acuerdos de intercambio.

13.2.3 Mensajería electrónica.

13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

14.1 Requisitos de seguridad de los sistemas de información.

14.1.1 Análisis y especificación de los requisitos de seguridad.

14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.

14.1.3 Protección de las transacciones por redes telemáticas.

14.2 Seguridad en los procesos de desarrollo y soporte.

14.2.1 Política de desarrollo seguro de software.

14.2.2 Procedimientos de control de cambios en los sistemas.

14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

14.2.4 Restricciones a los cambios en los paquetes de software.

14.2.5 Uso de principios de ingeniería en protección de sistemas.

14.2.6 Seguridad en entornos de desarrollo.

14.2.7 Externalización del desarrollo de software.

14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.

14.2.9 Pruebas de aceptación.

14.3 Datos de prueba.

14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.

15.1 Seguridad de la información en las relaciones con suministradores.

15.1.1 Política de seguridad de la información para suministradores.

15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.

15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.

15.2 Gestión de la prestación del servicio por suministradores.

Iso27000.es: Documento sólo para uso didáctico. La norma oficial debe adquirirse en las entidades autorizadas para su venta. Octubre-2013

(GESCONSULTOR, 2013)

CAPÍTULO III

PLAN DE AUDITORÍA

3.1 Alcance

Realizar una auditoría informática al sistema contable de la Unidad Educativa para el período 2017, basado en la norma ISO 27002 – Controles de Seguridad y elaboración de un informe con los resultados obtenidos.

3.2 Objetivos

Objetivo general:

- Auditar la seguridad informática al sistema contable de la unidad educativa La Asunción, para el período 2017.

Objetivos Específicos

- Investigar el ambiente relacionado con la seguridad informática del sistema contable en la unidad educativa.
- Estudiar las buenas prácticas de gestión de seguridad de la información basado en la Norma ISO 27002.
- Elaborar un plan de auditoría.
- Ejecutar la auditoría y emitir un informe, detallando los resultados de la misma, incluyendo las observaciones y sus respectivas recomendaciones.

3.3 Fuentes de información

1. El personal de la Unidad Educativa que proporcionó información durante la ejecución del trabajo, se detalla a continuación:

Tabla 1 Fuentes de información

NOMBRE	CARGO	ÁREA
Sra. Marcela Serrano	SECRETARIA	RECTORADO

Mg. Fanny Cobos	DIRECTORA FINANCIERA	DEPARTAMENTO CONTABLE-FINANCIERO
CPA. Samantha Ulloa	CONTADORA	DEPARTAMENTO CONTABLE-FINANCIERO
Tnlgo. María de Lourdes Crespo	AUXILIAR DE COLECTURÍA	DEPARTAMENTO CONTABLE-FINANCIERO
Sra. Mariela Barrera	GUARDA ALMACÉN	DEPARTAMENTO CONTABLE-FINANCIERO
Tnlgo. José Galarza	JEFE DEL DEPARTAMENTO	DEPARTAMENTO DE SISTEMAS
Mg. Janina Zuñiga	PROOGRAMADORA DE SISTEMAS	DEPARTAMENTO DE SISTEMAS

Realizado por: La autora

3.4 Cronograma de actividades

Ilustración 5 Cronograma de actividades

Realizado por: La autora

ACTIVIDADES	SEMANA 1					SEMANA 2					SEMANA 3					SEMANA 4					SEMANA 5					SEMANA 6					SEMANA 7					SEMANA 8					SEMANA 9					SEMANA 10				
	L	M	M	J	V	L	M	M	J	V	L	M	M	J	V	L	M	M	J	V	L	M	M	J	V	L	M	M	J	V	L	M	M	J	V	L	M	M	J	V	L	M	M	J	V	L	M	M	J	V
Conocimiento del sistema																																																			
Análisis de transacciones y recursos																																																		
Análisis de riesgos y amenazas																																																		
Análisis de controles																																																		
Evaluación de Controles																																																		
Informe de auditoría																																																		

3.5 Herramientas útiles para el desarrollo de la auditoría

- Cuestionario

El cuestionario es una herramienta basada en una serie de preguntas presentadas en una ficha, con la finalidad de que el auditor pueda obtener información del área auditada.

Ilustración 6 Modelo cuestionario de auditoría

UNIDAD EDUCATIVA LA ASUNCIÓN **CUESTIONARIO DE AUDITORÍA** **DEPARTAMENTO DE SISTEMAS**					
N°	**PREGUNTA**	**SI**	**NO**	**N/A**	**OBSERVACIONES**

Fecha:

Responsable: _____

_____

Realizado por: La autora

- Matriz de identificación de riesgos

Los riesgos identificados en cada uno de los 14 dominios serán detallados en la siguiente matriz:

Ilustración 7 Modelo matriz de identificación de riesgos

DOMINIO:	
RIESGOS	
R1	
R2	
….	

Realizado por: La autora

- Parámetros de evaluación y calificación de riesgos

La evaluación y calificación de riesgos se realizará en escalas de 3, considerando que bajo es de 1-3, medio de 4-6 y alto de 7-9

Ilustración 8 Parámetros de evaluación y calificación de riesgos

CALIFICACIÓN	**RIESGO TOTAL**
BAJO	1 – 3
MEDIO	4 – 6
ALTO	7 – 9

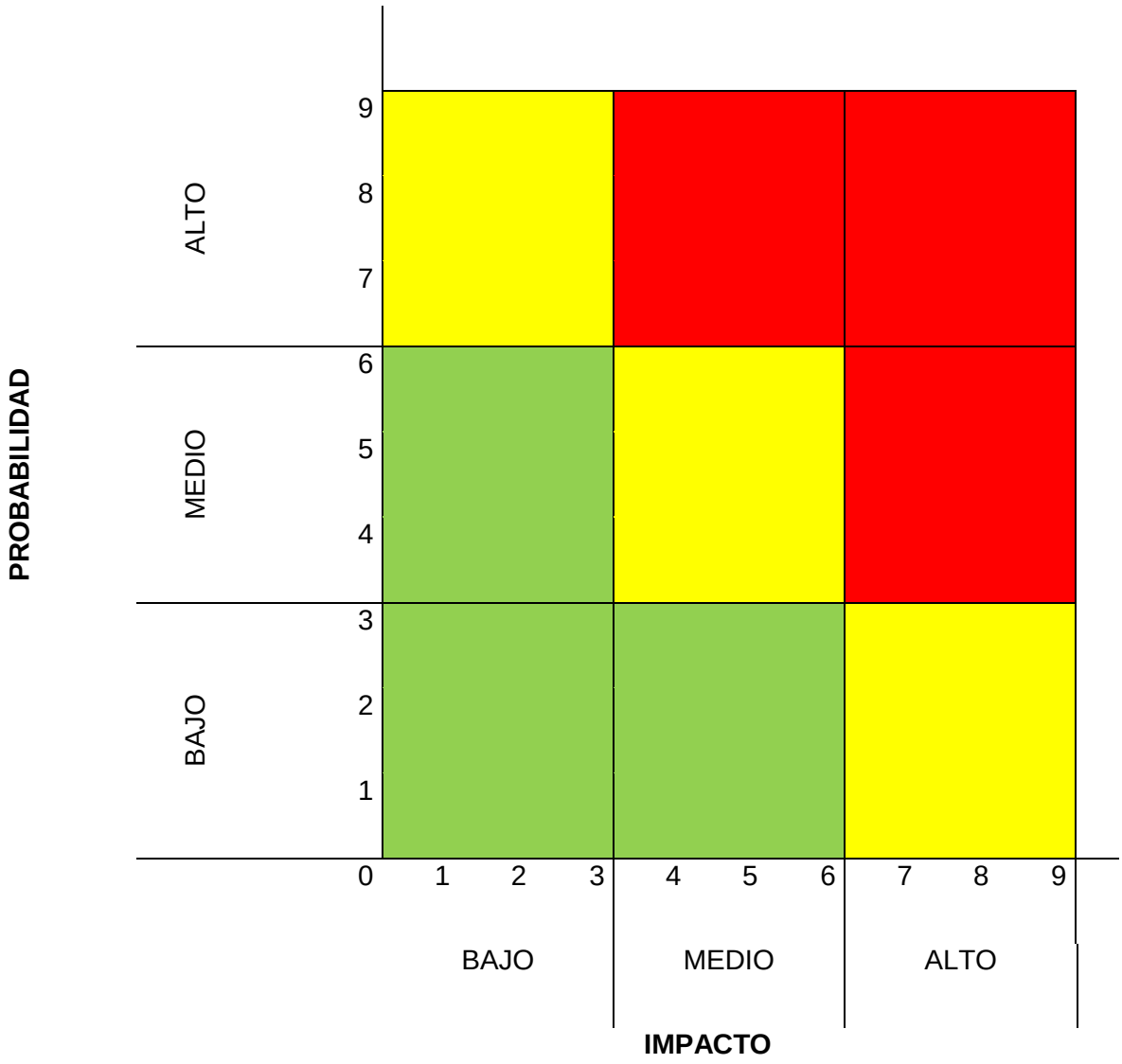
CALIFICACIÓN	**IDENTIFICACIÓN**
BAJO	
MEDIO	
ALTO	

Realizado por: La autora

- Matriz de evaluación y calificación de riesgos

La matriz de riesgos representa gráficamente en el eje de las ordenadas el impacto de los riesgos y en el eje de las abscisas la probabilidad, permitiendo evaluar de forma cualitativa dichos riesgos.

Ilustración 9 Modelo matriz de evaluación y calificación de riesgos



Realizado por: La autora

CAPÍTULO IV

EJECUCIÓN DE LA AUDITORÍA

4.1 Análisis de transacciones y recursos

Se realizó el cuestionario de auditoría al departamento de sistemas referente al departamento contable-financiero basado en la ISO 27002:2013, englobando los 14 dominios que contiene esta norma.

Tabla 2 Cuestionario de auditoría

UNIDAD EDUCATIVA LA ASUNCIÓN **CUESTIONARIO DE AUDITORÍA REALIZADO AL DEPARTAMENTO DE SISTEMAS REFERENTE AL DEPARTAMENTO FINANCIERO Y CONTABLE**					
N°	**PREGUNTA**	**SI**	**NO**	**N/A**	**OBSERVACIONES**
1	**POLÍTICAS DE SEGURIDAD**				
1	¿La Unidad Educativa tiene políticas para la seguridad de la información?			X	NO ESTÁN DEFINIDAS POR ESCRITO
2	¿La Unidad Educativa cuenta con un Responsable de Seguridad de la información?	X			NO EXCLUSIVAMENTE PERO TODOS SOMOS CUSTODIOS DE LA INFORMACIÓN
3	¿Las políticas para la seguridad de la información están aprobadas por la dirección, publicadas y comunicadas a los empleados?		X		
4	¿ Las políticas para la seguridad de la información son revisadas con regularidad, y tienen mejoras significativas para garantizar su idoneidad, adecuación y efectividad?			X	
2	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN**				
5	¿Existe una clara definición y asignación de responsabilidades para SI?		X		

6	¿Se tienen definido un comité donde traten la Seguridad de la Información?		X		EL DPTO DE SISTEMAS CONSTA DE 3 PERSONAS, ES UNA EMPRESA PEQUEÑA
7	La persona responsable de SI o el gobierno IT tienen contacto con expertos de SI?			X	NO EXISTE UN RESPONSABLE ESPECÍFICO
8	¿En la gestión de proyectos se toma en cuenta la Seguridad de la Información?	X			
9	¿Se adoptan medidas de seguridad de la información adecuadas para la protección contra los riesgos derivados del uso de los recursos móviles?	X			
10	¿Se ha implementado una política y medidas de seguridad de apoyo para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas al teletrabajo?			X	EL TELETRABAJO SOLO ES REALIZADO POR EL PERSONAL ADMINISTRATIVO
3	**SEGURIDAD LIGADA A LOS RECURSOS**				
11	¿Se realizan revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes?			X	LOS CANDIDATOS ES UN PROCESO DE TALENTO HUMANO
12	¿Los empleados, contratistas y terceros aceptan y firman los términos y condiciones del contrato de empleo, el cual se establecen sus obligaciones y las obligaciones de la Unidad Educativa para la seguridad de información?	X			
13	¿La Dirección requiere a empleados, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los procedimientos?	X			
14	¿ Todos los empleados de la Unidad Educativa , contratistas y usuarios de terceros reciben entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales y de seguridad de la información relevantes para la función de su trabajo?		X		
15	¿Existen políticas y un proceso formal disciplinario de seguridad de la información comunicado a empleados, y monitoreo de cumplimiento?		X		
16	¿Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste están claramente definidas, comunicadas a empleado o contratista y asignadas efectivamente?			X	

4	**GESTIÓN DE ACTIVOS**				
17	¿Todos los activos (activos de información) están claramente identificados?	X			
18	¿Todos los activos (activos de la información) tienen asignado su responsable, así como su uso aceptable, incluyendo la devolución de los mismos? Manejo de acuerdo a las regulaciones para el uso adecuado de la información?	X			
20	¿ La información se encuentra clasificada en relación a su valor, requisitos legales, sensibilidad y criticidad para la Unidad Educativa?	X			
21	¿Se ha desarrollado e implementado un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la Unidad Educativa?	X			DEPARTAMENTO DE COMPRAS REALIZA ESTE PROCESO
22	¿Se ha desarrollado e implementado procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la Unidad Educativa?			X	
23	¿Se han establecido procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la Unidad Educativa.?			X	
24	¿Se han protegido los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la Unidad Educativa?	X			
5	**CONTROL DE ACCESOS**				
25	¿Se han establecido, documentado, revisado y aprobado una política de control de accesos en base a las necesidades de seguridad y de negocio de la Unidad Educativa?		X		FALTA DOCUMENTACIÓN FORMAL
26	¿Existe un control de acceso a las redes y servicios asociados?	X			
27	¿Existe un procedimiento formal de altas y bajas de usuarios con objeto de habilitar la asignación de derechos de acceso?		X		EL PROCEDIMIENTO EXISTE PERO NO ES FORMAL
28	¿Se ha implementado un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios?		X		EL PROCEDIMIENTO EXISTE PERO NO ES FORMAL

29	¿La asignación y uso de derechos de acceso con privilegios especiales son restringidos y controlados?	x			
30	¿ La asignación de información confidencial para la autenticación es supervisada mediante un proceso de gestión controlado?	x			
31	¿Son retirados los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o son revisados en caso de cambio?	x			
32	¿Se exige a los usuarios el uso de las buenas prácticas de seguridad en el uso de información confidencial para la autenticación?			x	
33	¿Se restringe el acceso a los usuarios y al personal de mantenimiento de sistemas y aplicaciones, en relación a la política de control de accesos definida?	x			
34	¿Tienen procedimientos seguros de inicio de sesión?	x			
35	¿Tienen un manejo adecuado de gestión de contraseñas de usuario?		x		FALTA ENCRIPTACIÓN
36	¿Se dispone de herramientas de administración de sistemas y estas son restringidas y estrechamente controladas?	X			
37	¿Existe una restricción del acceso al código fuente de las aplicaciones software?	X			
6	**CIFRADO**				
38	¿Se ha desarrollado e implementado una política que regule el uso de controles criptográficos (cifrado) para la protección de la información?		X		
39	¿Se ha desarrollado e implementado una política de gestión de claves criptográficas a través de todo su ciclo de vida?		X		
7	**SEGURIDAD FÍSICA Y AMBIENTAL**				
40	¿Se ha definido y utilizado perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica?	X			
41	¿Las áreas seguras están protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso?	X			

42	¿Se ha diseñado y aplicado un sistema de seguridad física a las oficinas, salas e instalaciones de los departamentos contable-financiero y sistemas?		X		
43	¿Se ha diseñado y aplicado una protección física/lógica contra desastres naturales, ataques maliciosos o accidentes?		X		
44	¿Se ha diseñado y aplicado procedimientos para el desarrollo de trabajos y actividades en áreas seguras?		X		
45	¿Se tiene definido áreas de acceso restringido y los mismos son controlados su acceso?	X			
46	¿Los equipos se han reemplazado y protegido para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado?	X			DE ACCESO NO AUTORIZADO SI, DE AMENAZAS Y RIESGOS AMBIENTALES NO
47	¿Los equipos están protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo?	X			LOS DEL PERSONAL ADMINISTRATIVO Y SERVIDORES
48	¿Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información están protegidos contra la intercepción, interferencia o posibles daños?	X			EN PARTE, FALTA MEJORAS EN LA INFRAESTRUCTURA
49	¿Los equipos se mantienen adecuadamente con el objeto de garantizar su disponibilidad e integridad continua? ¿Existe una bitácora de este mantenimiento?	X			SE DA MANTENIMIENTO, DEBE IMPLEMENTARSE MEJORAS EN LA BITACORA
50	¿Existe y se acciona procedimientos para la salida de equipos, así como su uso fuera de las instalaciones e igualmente para la re-integración a la oficina?		X		NO EXISTE EL PROCEDIMIENTO, PERO LA SALIDA DE EQUIPOS ESTA PROHIBIDA
51	¿Se verifican todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización?	X			
52	¿Tienen política de puesto de trabajo despejado y bloqueo de pantalla?		X		
8	**SEGURIDAD EN LA OPERATIVA**				
53	¿Se documentan y aprueban los procedimientos operativos y se dejan a disposición de todos los usuarios que los necesiten?		X		

54	¿Tienen un manejo adecuado de cambios que afectan a la seguridad de la información en la Unidad Educativa y procesos de negocio, las instalaciones y sistemas de procesamiento de información?		X		
55	¿ Se cuenta con entornos de desarrollo, pruebas y operacionales separados y debidamente controlado su acceso para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional?	X			ESTO ES GRACIAS A LA UNIVERSIDAD DEL AZUAY EN LA PARTE DE SOFTWARE
56	¿Se ha implementado controles para la detección, prevención y recuperación ante afectaciones de malware y/o ataques de seguridad informática en combinación con la concientización adecuada de los usuarios?	X			
57	¿Se realiza pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida?	X			
58	¿Se maneja un registro y gestión adecuado de eventos (logs)?		X		
59	¿Se protege contra posibles alteraciones y accesos no autorizados la información de los registros?	X			
60	¿Se registran las actividades del administrador, del operador del sistema y los registros asociados son revisados de manera regular?	X			EN EL SISTEMA DE CORREO ELECTRÓNICO
61	¿Se sincronizan los relojes de todos los sistemas de procesamiento de información pertinentes?	X			
62	¿Se han implementado procedimientos para controlar la instalación de software en sistemas operacionales?	X			
63	¿Se han establecido e implementado reglas que rigen la instalación de software por parte de los usuarios?	X			LOS USUARIOS NO PUEDEN INSTALAR
64	¿Se han planificado y acordado los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales?		X		
9	**SEGURIDAD DE LAS TELECOMUNICACIONES**				
65	¿Se administran y controlan las redes para proteger la información en sistemas y aplicaciones?	X			

66	¿Se han identificado mecanismos de seguridad para los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados?	X			
67	¿La redes se segregan en función de los grupos de servicios, usuarios y sistemas de información?	X			
68	¿Existen políticas, procedimientos y controles formales de transferencia información que viaja a través del uso de todo tipo de medios de comunicación?	X			EL PROCEDIMIENTO EXISTE PERO NO ES FORMAL
69	¿Existen acuerdos de intercambio de la información?		X		
70	¿Se identifica, revisa y documenta de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la Unidad Educativa para la protección de información?		X		
10	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**				
71	¿ Los requisitos relacionados con la seguridad de la información se incluyen en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes?	X			
72	¿ La información de los servicios de aplicación que pasan a través de redes públicas se protegen contra actividades fraudulentas, de modificación no autorizada?	X			
73	¿La información en transacciones de servicios de aplicación se protegen para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción?	X			
74	¿Se establecen y aplican reglas para el desarrollo de software (código seguro, estático y dinámico) y sistemas dentro de la Unidad Educativa?	X			
75	¿Existen políticas de seguridad para las actividades de desarrollo del sistema que se hayan externalizado y se supervisa su cumplimiento?		X		
76	¿Se realiza pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo?	X			

77	¿Se establecen programas de prueba "funcionales" y criterios relacionados para la "aceptación" de nuevos sistemas de información, actualizaciones y/o nuevas versiones?	X			
78	¿Existe políticas de manejo de datos de pruebas y se protegen y controlan?	X			
11	**RELACIONES CON SUMINISTRADORES**				
79	¿Se acuerda y documenta y aprueba adecuadamente los requisitos de seguridad de la información requeridos por los activos de la Unidad Educativa con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas?	X			
80	¿Se establecen todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información?	X			
81	¿ Los acuerdos con los proveedores incluyen los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones?			X	
82	¿El departamento de sistemas monitorea, revisa y audita la presentación de servicios del proveedor?		X		
83	¿Se administran los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos?		X		
12	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**				
84	¿ Se establecen las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información?	X			
85	¿La notificación de eventos de seguridad de la información se informan lo antes posible utilizando los canales de administración adecuados?	X			
86	¿Se requiere notificar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la Unidad Educativa?	X			SE ESTRUCUTRÓ EL TEMA DE SEGURIDAD CON UN CANAL VPN PARA INGRESE A LOS SISTEMAS EXTERNAMENTE

87	¿ Se evalúa los eventos de seguridad de la información y se decide su clasificación como incidentes?		X		
88	¿Se tiene definido políticas y procedimientos de respuesta ante los incidentes de seguridad de la información en atención a los procedimientos documentados?		X		
89	¿ Se utiliza el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro?		X		
90	¿El departamento define y aplica los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia?		X		
13	**ASPECTOS DE SI EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**				
91	¿La Unidad Educativa determinó los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre?		X		
92	¿La Unidad Educativa establece, documenta, implementa y mantiene los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas?		X		
93	¿El departamento verifica regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas?	X			
94	¿Se cuenta con instalaciones de procesamiento de la información redundantes para ser usadas en caso de una contingencia?	X			NO SON INSTALACIONES SINO UN SERVIDOR
14	**CUMPLIMIENTO**				
95	¿Se han identificado, documentado y mantienen actualizados y de manera explícita para cada sistema de información y para la Unidad Educativa todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la Unidad Educativa para cumplir con estos requisitos?		X		
96	¿Se han implementado procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software originales?	X			LAS LICENCIAS SE OBTIENEN DE LA UDA

97	¿ Los registros son protegidos contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales?	X			
98	¿ Se garantiza la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan?	X			
99	¿Se utilizan controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas?		X		
100	¿Los jefes de área revisan regularmente el cumplimiento de políticas y procedimientos de seguridad de la información dentro de su área de responsabilidad?		X		
101	¿Existe una revisión y comprobación de las políticas y procedimientos de seguridad de la información a nivel Organizacional por parte del Responsable de Seguridad de la Información de la Unidad Educativa?			X	NO EXISTE UN RESPONSABLE ESPECÍFICO

Fecha:	21/08/2017- 23/8/2017- 24/08/2017
Responsable:	JOSÉ GALARZA - JANINA ZUÑIGA - ALÍ MENDEZ

Realizado por: La autora

4.2 Identificación de riesgos y amenazas

Los riesgos y amenazas se han ido identificando en cada uno de los 14 dominios que presenta la norma ISO 27002 y se presentan a continuación:

Tabla 3 Identificación de riesgos y amenazas - Políticas de seguridad

DOMINIO:	**POLÍTICAS DE SEGURIDAD**
DESCRIPCIÓN	
RIESGO 1 **Incumplimiento**	La Unidad Educativa no tiene un documento que determine las políticas de seguridad de la información
RIESGO 2 **Incumplimiento**	No existe la asignación de un responsable de seguridad de la información dentro del departamento de sistemas
RIESGO 3 **Incumplimiento**	Las políticas para la seguridad de la información no están aprobadas por la dirección, publicadas, ni comunicadas a los empleados.
RIESGO 4 **Incumplimiento**	Las políticas para la seguridad de la información al no estar redactadas en un documento no pueden ser revisadas con regularidad, y buscar mejoras significativas para garantizar su idoneidad, adecuación y efectividad.

Realizado por: La autora

Tabla 4 Identificación de riesgos y amenazas - Aspectos organizativos de la seguridad de la información

DOMINIO:	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN**
DESCRIPCIÓN	
RIESGO 5 **Error y/o** **Fraude**	No existe una clara definición y asignación de responsabilidades para seguridad de la información

RIESGO 6 **Error y/o** **Fraude**	No se tiene definido un comité donde traten la seguridad de la información
RIESGO 7 **Error y/o** **Fraude**	Al no existir un responsable específico de SI o el gobierno IT, tampoco se tiene contacto con expertos de SI
RIESGO 8 **Incumplimiento**	La SI en relación a la gestión de proyectos no presenta un documento escrito que respalde la protección de la información.
RIESGO 9 **Incumplimiento**	La SI en relación al uso de recursos móviles no presenta un documento escrito que respalde la protección de la información.
RIESGO 10 **Incumplimiento**	No se ha implementado una política y medidas de seguridad de apoyo para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas al teletrabajo

Realizado por: La autora

Tabla 5 Identificación de riesgos y amenazas - Seguridad ligada a los recursos

DOMINIO:	**SEGURIDAD LIGADA A LOS RECURSOS**
DESCRIPCIÓN	
RIESGO 11 **Error y/o** **Fraude**	No se archivan controles de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes
RIESGO 12	Todos los empleados de la Unidad Educativa , contratistas y usuarios de terceros no reciben entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y

Error y/o Fraude	procedimientos organizacionales y de seguridad de la información relevantes para la función de su trabajo
RIESGO 13 Incumplimiento	No existen políticas y un proceso formal disciplinario de seguridad de la información comunicado a empleados, y monitoreo de cumplimiento
RIESGO 14 Error y/o Fraude	Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste no están claramente definidas, comunicadas a empleado o contratista y asignadas efectivamente.

Realizado por: La autora

Tabla 6 Identificación de riesgos y amenazas - Gestión de activos

DOMINIO:	**GESTIÓN DE ACTIVOS**
DESCRIPCIÓN	
RIESGO 15 Error y/o Fraude	No se aplica un desarrollo e implementación de procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la Unidad Educativa
RIESGO 16 Error y/o Fraude	No se aplica procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la Unidad Educativa.

Realizado por: La autora

Tabla 7 Identificación de riesgos y amenazas - Control de accesos

DOMINIO:	**CONTROL DE ACCESOS**
DESCRIPCIÓN	

RIESGO 17 Incumplimiento	No se han establecido, documentado, revisado y aprobado una política de control de accesos en base a las necesidades de seguridad y de negocio de la Unidad Educativa
RIESGO 18 Incumplimiento	No se existe un procedimiento formal de altas y bajas de usuarios con objeto de habilitar la asignación de derechos de acceso.
RIESGO 19 Incumplimiento	No se ha implementado un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios
RIESGO 20 Error y/o Fraude	No se exige a los usuarios el uso de las buenas prácticas de seguridad en el uso de información confidencial para la autenticación
RIESGO 21 Error y/o Fraude	No tienen un manejo adecuado de gestión de contraseñas de usuario

Realizado por: La autora

Tabla 8 Identificación de riesgos y amenazas - Cifrado

DOMINIO:	**CIFRADO**
DESCRIPCIÓN	
RIESGO 22 Incumplimiento	No se ha desarrollado e implementado una política que regule el uso de controles criptográficos (cifrado) para la protección de la información
RIESGO 23 Incumplimiento	No se ha desarrollado e implementado una política de gestión de claves criptográficas a través de todo su ciclo de vida

Realizado por: La autora

Tabla 9 Identificación de riesgos y amenazas - Seguridad física y ambiental

DOMINIO:	**SEGURIDAD FÍSICA Y AMBIENTAL**
DESCRIPCIÓN	
RIESGO 24 Deterioro	No se ha diseñado y aplicado un sistema de seguridad física a las oficinas, salas e instalaciones de los departamentos contable-financiero y sistemas
RIESGO 25 Deterioro	No se ha diseñado y aplicado una protección física/lógica contra desastres naturales, ataques maliciosos o accidentes
RIESGO 26 Incumplimiento	No se ha diseñado y aplicado procedimientos para el desarrollo de trabajos y actividades en áreas seguras
RIESGO 27 Deterioro	Los equipos no se han reemplazado y protegido para reducir los riesgos de las amenazas y peligros ambientales
RIESGO 28 Deterioro	Falta diseñar una infraestructura adecuada para que los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se encuentren protegidos contra la intercepción, interferencia o posibles daños
RIESGO 29 Deterioro	Falta actualizar la bitácora para que los equipos se mantengan adecuadamente y poder garantizar su disponibilidad e integridad continua.
RIESGO 30 Incumplimiento	No existe una política de puesto de trabajo despejado y bloqueo de pantalla

Realizado por: La autora

Tabla 10 Identificación de riesgos y amenazas - Seguridad en la operativa

DOMINIO:	**SEGURIDAD EN LA OPERATIVA**
RIESGOS	
RIESGO 31 Incumplimiento	No se documentan y aprueban los procedimientos operativos.
RIESGO 32 Error y/o fraude	No tienen un manejo adecuado de cambios que afectan a la seguridad de la información en la Unidad Educativa y procesos de negocio, las instalaciones y sistemas de procesamiento de información
RIESGO 33 Error y/o fraude	No se maneja un registro y gestión adecuado de eventos (logs)
RIESGO 34 Incumplimiento	No se han planificado y acordado los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales

Realizado por: La autora

Tabla 11 Identificación de riesgos y amenazas - Seguridad de telecomunicaciones

DOMINIO:	**SEGURIDAD DE LAS TELECOMUNICACIONES**
RIESGOS	
RIESGO 35 Incumplimiento	No existe un documento de políticas, procedimientos y controles formales de transferencia información que viaja a través del uso de todo tipo de medios de comunicación
RIESGO 36 Incumplimiento	No existen acuerdos de intercambio de la información

RIESGO 37 **Error y/o fraude**	No se identifica, revisa y documenta de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la Unidad Educativa para la protección de información

Realizado por: La autora

Tabla 12 Identificación de riesgos y amenazas - Adquisición, desarrollo y mantenimiento de los sistemas de información

DOMINIO:	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**
RIESGOS	
RIESGO 38 **Incumplimiento**	No existen políticas de seguridad para las actividades de desarrollo del sistema que se hayan externalizado y se supervisa su cumplimiento

Realizado por: La autora

Tabla 13 Identificación de riesgos y amenazas – Relaciones con suministradores

DOMINIO:	**RELACIONES CON SUMINISTRADORES**
RIESGOS	
RIESGO 39 **Incumplimiento**	Los acuerdos con los proveedores no incluyen los requisitos para abordar los riesgos de seguridad de la información

	asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones
RIESGO 40 Erro y/o fraude	El departamento de sistemas no monitorea, revisa y audita la presentación de servicios del proveedor
RIESGO 41 Incumplimiento	No se administran los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos

Realizado por: La autora

Tabla 14 Identificación de riesgos y amenazas – Gestión de incidentes en la seguridad de la información

DOMINIO:	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**
RIESGOS	
RIESGO 42 Error y/o fraude	No se evalúa los eventos de seguridad de la información y se decide su clasificación como incidentes
RIESGO 43 Incumplimiento	No se tiene definido políticas y procedimientos de respuesta ante los incidentes de seguridad de la información en atención a los procedimientos documentados
RIESGO 44 Incumplimiento	No se utiliza el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro

RIESGO 45 Incumplimiento	El departamento no define y aplica los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia

Realizado por: La autora

Tabla 15 Identificación de riesgos y amenazas – Aspectos de SI en la gestión de la continuidad del negocio

DOMINIO:	**ASPECTOS DE SI EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**
RIESGOS	
RIESGO 46 Deterioro	La Unidad Educativa no ha determinado los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre
RIESGO 47 Deterioro	La Unidad Educativa no establece, documenta, implementa, ni mantiene los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas

Realizado por: La autora

Tabla 16 Identificación de riesgos y amenazas - Cumplimiento

DOMINIO:	**CUMPLIMIENTO**
RIESGOS	
RIESGO 48 Incumplimiento	No se han identificado, documentado, ni se mantienen actualizados y de manera explícita para cada sistema de información y para la Unidad Educativa todos los requisitos

	estatutarios, normativos y contractuales legislativos junto al enfoque de la Unidad Educativa para cumplir con estos requisitos
RIESGO 49 Error y/o fraude	No se utilizan controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas
RIESGO 50 Incumplimiento	Por falta de documentación los jefes de área no pueden revisar regularmente el cumplimiento de políticas y procedimientos de seguridad de la información dentro de su área de responsabilidad.
RIESGO 51 Error y/o fraude	Al no existir un responsable de la SI no existe una revisión y comprobación de las políticas y procedimientos de seguridad de la información a nivel Organizacional

Realizado por: La autora

4.3 Evaluación y calificación del riesgo

La evaluación y calificación de los riesgos se han realizado de acuerdo a la probabilidad de ocurrencia y el impacto que producirían los mismos. El total se obtiene del producto entre probabilidad e impacto.

Tabla 17 Evaluación y calificación de riesgos

EVALUACIÓN Y CALIFICACIÓN DE LOS RIESGOS					
DOMINIO	**DESCRIPCIÓN**	**RIESGO**	**PROBABILIDAD**	**IMPACTO**	**TOTAL**
POLÍTICAS DE SEGURIDAD	La Unidad Educativa no tiene un documento que determine las políticas de seguridad de la información	**RIESGO 1 Incumplimiento**	8	9	72
	No existe la asignación de un responsable de seguridad de la información dentro del departamento de sistemas	**RIESGO 2 Incumplimiento**	7	7	49
	Las políticas para la seguridad de la información no están aprobadas por la dirección, publicadas, ni comunicadas a los empleados.	**RIESGO 3 Incumplimiento**	8	8	64
	Las políticas para la seguridad de la información al no estar redactadas en un documento no pueden ser revisadas con regularidad, y buscar mejoras significativas para garantizar su idoneidad, adecuación y efectividad.	**RIESGO 4 Incumplimiento**	8	7	56
	No existe una clara definición y asignación de responsabilidades para seguridad de la información	**RIESGO 5 Error y/o Fraude**	8	7	56

ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	No se tiene definido un comité donde traten la seguridad de la información	**RIESGO 6 Error y/o Fraude**	7	6	42
	Al no existir un responsable específico de SI o el gobierno IT, tampoco se tiene contacto con expertos de SI	**RIESGO 7 Error y/o Fraude**	5	5	25
	La SI en relación a la gestión de proyectos no presenta un documento escrito que respalde la protección de la información.	**RIESGO 8 Incumplimiento**	5	4	20
	La SI en relación al uso de recursos móviles no presenta un documento escrito que respalde la protección de la información.	**RIESGO 9 Incumplimiento**	2	3	6
	No se ha implementado una política y medidas de seguridad de apoyo para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas al teletrabajo	**RIESGO 10 Incumplimiento**	7	8	56
	No se archivan controles de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes	**RIESGO 11 Error y/o Fraude**	6	7	42

SEGURIDAD LIGADA A LOS RECURSOS	Todos los empleados de la Unidad Educativa, contratistas y usuarios de terceros no reciben entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales y de seguridad de la información relevantes para la función de su trabajo	**RIESGO 12 Error y/o Fraude**	8	7	56
	No existen políticas y un proceso formal disciplinario de seguridad de la información comunicado a empleados, y monitoreo de cumplimiento	**RIESGO 13 Incumplimiento**	7	7	49
	Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste no están claramente definidas, comunicadas a empleado o contratista y asignadas efectivamente.	**RIESGO 14 Error y/o Fraude**	7	7	49
GESTIÓN DE ACTIVOS	No se aplica un desarrollo e implementación de procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la Unidad Educativa	**RIESGO 15 Error y/o Fraude**	6	7	42
	No se aplica procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la Unidad Educativa.	**RIESGO 16 Error y/o Fraude**	6	7	42

CONTROL DE ACCESOS	No se han establecido, documentado, revisado y aprobado una política de control de accesos en base a las necesidades de seguridad y de negocio de la Unidad Educativa	**RIESGO 17 Incumplimiento**	7	8	56
	No se existe un procedimiento formal de altas y bajas de usuarios con objeto de habilitar la asignación de derechos de acceso.	**RIESGO 18 Incumplimiento**	7	8	56
	No se ha implementado un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios	**RIESGO 19 Incumplimiento**	7	8	56
	No se exige a los usuarios el uso de las buenas prácticas de seguridad en el uso de información confidencial para la autenticación	**RIESGO 20 Error y/o Fraude**	7	8	56
	No tienen un manejo adecuado de gestión de contraseñas de usuario	**RIESGO 21 Error y/o Fraude**	8	9	72
CIFRADO	No se ha desarrollado e implementado una política que regule el uso de controles criptográficos (cifrado) para la protección de la información	**RIESGO 22 Incumplimiento**	9	9	81

	No se ha desarrollado e implementado una política de gestión de claves criptográficas a través de todo su ciclo de vida	**RIESGO 23 Incumplimiento**	9	9	81
SEGURIDAD FÍSICA Y AMBIENTAL	No se ha diseñado y aplicado un sistema de seguridad física a las oficinas, salas e instalaciones de los departamentos contable-financiero y sistemas	**RIESGO 24 Deterioro**	9	9	81
	No se ha diseñado y aplicado una protección física/lógica contra desastres naturales, ataques maliciosos o accidentes	**RIESGO 25 Deterioro**	9	9	81
	No se ha diseñado y aplicado procedimientos para el desarrollo de trabajos y actividades en áreas seguras	**RIESGO 26 Incumplimiento**	9	9	81
	Los equipos no se han reemplazado y protegido para reducir los riesgos de las amenazas y peligros ambientales	**RIESGO 27 Deterioro**	9	9	81
	Falta diseñar una infraestructura adecuada para que los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se encuentren protegidos contra la intercepción, interferencia o posibles daños	**RIESGO 28 Deterioro**	8	7	56
	Falta actualizar la bitácora para que los equipos se mantengan adecuadamente y poder garantizar su disponibilidad e integridad continua.	**RIESGO 29 Deterioro**	8	7	56

	No existe una política de puesto de trabajo despejado y bloqueo de pantalla	**RIESGO 30 Incumplimiento**	4	5	20
SEGURIDAD EN LA OPERATIVA	No se documentan y aprueban los procedimientos operativos.	**RIESGO 31 Incumplimiento**	5	6	30
	No tienen un manejo adecuado de cambios que afectan a la seguridad de la información en la Unidad Educativa y procesos de negocio, las instalaciones y sistemas de procesamiento de información	**RIESGO 32 Error y/o fraude**	5	6	30
	No se maneja un registro y gestión adecuado de eventos (logs)	**RIESGO 33 Error y/o fraude**	8	7	56
	No se han planificado y acordado los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales	**RIESGO 34 Incumplimiento**	7	6	42
SEGURIDAD DE LAS TELECOMUNICACIONES	No existe un documento de políticas, procedimientos y controles formales de transferencia información que viaja a través del uso de todo tipo de medios de comunicación	**RIESGO 35 Incumplimiento**	7	8	56
	No existen acuerdos de intercambio de la información	**RIESGO 36 Incumplimiento**	7	7	49

	No se identifica, revisa y documenta de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la Unidad Educativa para la protección de información	**RIESGO 37 Error y/o fraude**	8	8	64
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	No existen políticas de seguridad para las actividades de desarrollo del sistema que se hayan externalizado y se supervisa su cumplimiento	**RIESGO 38 Incumplimiento**	8	8	64
RELACIONES CON SUMINISTRADORES	Los acuerdos con los proveedores no incluyen los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones	**RIESGO 39 Incumplimiento**	7	8	56
	El departamento de sistemas no monitorea, revisa y audita la presentación de servicios del proveedor	**RIESGO 40 Erro y/o fraude**	9	8	72
	No se administran los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos	**RIESGO 41 Incumplimiento**	9	8	72

GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	No se evalúa los eventos de seguridad de la información y se decide su clasificación como incidentes	**RIESGO 42 Error y/o fraude**	9	8	72
	No se tiene definido políticas y procedimientos de respuesta ante los incidentes de seguridad de la información en atención a los procedimientos documentados	**RIESGO 43 Incumplimiento**	9	8	72
	No se utiliza el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro	**RIESGO 44 Incumplimiento**	9	8	72
	El departamento no define y aplica los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia	**RIESGO 45 Incumplimiento**	9	8	72
ASPECTOS DE SI EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	La Unidad Educativa no ha determinado los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre	**RIESGO 46 Deterioro**	9	9	81
	La Unidad Educativa no establece, documenta, implementa, ni mantiene los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas	**RIESGO 47 Deterioro**	9	9	81

CUMPLIMIENTO	No se han identificado, documentado, ni se mantienen actualizados y de manera explícita para cada sistema de información y para la Unidad Educativa todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la Unidad Educativa para cumplir con estos requisitos	**RIESGO 48 Incumplimiento**	8	9	72
	No se utilizan controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas	**RIESGO 49 Error y/o fraude**	9	8	72
	Por falta de documentación los jefes de área no pueden revisar regularmente el cumplimiento de políticas y procedimientos de seguridad de la información dentro de su área de responsabilidad.	**RIESGO 50 Incumplimiento**	8	8	64
	Al no existir un responsable de la SI no existe una revisión y comprobación de las políticas y procedimientos de seguridad de la información a nivel Organizacional	**RIESGO 51 Error y/o fraude**	9	8	72

Realizado por: La autora

Tabla 18 Ponderación de los riesgos

PONDERACIÓN DE LOS RIESGOS				
DESCRIPCIÓN	**RIESGO**	**PROBABILIDAD**	**IMPACTO**	**TOTAL**
No se ha desarrollado e implementado una política que regule el uso de controles criptográficos (cifrado) para la protección de la información	RIESGO 22 Incumplimiento	9	9	81
No se ha desarrollado e implementado una política de gestión de claves criptográficas a través de todo su ciclo de vida	RIESGO 23 Incumplimiento	9	9	81
No se ha diseñado y aplicado un sistema de seguridad física a las oficinas, salas e instalaciones de los departamentos contable-financiero y sistemas	RIESGO 24 Deterioro	9	9	81
No se ha diseñado y aplicado una protección física/lógica contra desastres naturales, ataques maliciosos o accidentes	RIESGO 25 Deterioro	9	9	81
No se ha diseñado y aplicado procedimientos para el desarrollo de trabajos y actividades en áreas seguras	RIESGO 26 Incumplimiento	9	9	81
Los equipos no se han reemplazado y protegido para reducir los riesgos de las amenazas y peligros ambientales	RIESGO 27 Deterioro	9	9	81
La Unidad Educativa no ha determinado los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre	RIESGO 46 Deterioro	9	9	81
La Unidad Educativa no establece, documenta, implementa, ni mantiene los procesos,	RIESGO 47 Deterioro	9	9	81

procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas				
La Unidad Educativa no tiene un documento que determine las políticas de seguridad de la información	RIESGO 1 Incumplimiento	8	9	72
No tienen un manejo adecuado de gestión de contraseñas de usuario	RIESGO 21 Error y/o fraude	8	9	72
El departamento de sistemas no monitorea, revisa y audita la presentación de servicios del proveedor	RIESGO 40 Error y/o fraude	9	8	72
No se administran los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos	RIESGO 41 Incumplimiento	9	8	72
No se evalúa los eventos de seguridad de la información y se decide su clasificación como incidentes	RIESGO 42 Error y/o fraude	9	8	72
No se tiene definido políticas y procedimientos de respuesta ante los incidentes de seguridad de la información en atención a los procedimientos documentados	RIESGO 43 Incumplimiento	9	8	72
No se utiliza el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro	RIESGO 44 Incumplimiento	9	8	72

El departamento no define y aplica los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia	RIESGO 45 Incumplimiento	9	8	72
No se han identificado, documentado, ni se mantienen actualizados y de manera explícita para cada sistema de información y para la Unidad Educativa todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la Unidad Educativa para cumplir con estos requisitos	RIESGO 48 Incumplimiento	8	9	72
No se utilizan controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas	RIESGO 49 Error y/o fraude	9	8	72
Al no existir un responsable de la SI no existe una revisión y comprobación de las políticas y procedimientos de seguridad de la información a nivel Organizacional	RIESGO 51 Error y/o fraude	9	8	72
Las políticas para la seguridad de la información no están aprobadas por la dirección, publicadas, ni comunicadas a los empleados.	RIESGO 3 Incumplimiento	8	8	64
No se identifica, revisa y documenta de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la Unidad Educativa para la protección de información	RIESGO 37 Error y/o fraude	8	8	64

No existen políticas de seguridad para las actividades de desarrollo del sistema que se hayan externalizado y se supervisa su cumplimiento	RIESGO 38 Incumplimiento	8	8	64
Por falta de documentación los jefes de área no pueden revisar regularmente el cumplimiento de políticas y procedimientos de seguridad de la información dentro de su área de responsabilidad.	RIESGO 50 Incumplimiento	8	8	64
Las políticas para la seguridad de la información al no estar redactadas en un documento no pueden ser revisadas con regularidad, y buscar mejoras significativas para garantizar su idoneidad, adecuación y efectividad.	RIESGO 4 Incumplimiento	8	7	56
No existe una clara definición y asignación de responsabilidades para seguridad de la información	RIESGO 5 Error y/o Fraude	8	7	56
No se ha implementado una política y medidas de seguridad de apoyo para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas al teletrabajo	RIESGO 10 Incumplimiento	7	8	56
Todos los empleados de la Unidad Educativa, contratistas y usuarios de terceros no reciben entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales y de seguridad de la información relevantes para la función de su trabajo	RIESGO 12 Error y/o fraude	8	7	56
No se han establecido, documentado, revisado y aprobado una política de control de accesos en	RIESGO 17 Incumplimiento	7	8	56

base a las necesidades de seguridad y de negocio de la Unidad Educativa				
No se existe un procedimiento formal de altas y bajas de usuarios con objeto de habilitar la asignación de derechos de acceso.	RIESGO 18 Incumplimiento	7	8	56
No se ha implementado un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios	RIESGO 19 Incumplimiento	7	8	56
No se exige a los usuarios el uso de las buenas prácticas de seguridad en el uso de información confidencial para la autenticación	RIESGO 20 Error y/o fraude	7	8	56
Falta diseñar una infraestructura adecuada para que los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se encuentren protegidos contra la intercepción, interferencia o posibles daños	RIESGO 28 Deterioro	8	7	56
Falta actualizar la bitácora para que los equipos se mantengan adecuadamente y poder garantizar su disponibilidad e integridad continua.	RIESGO 29 Deterioro	8	7	56
No se maneja un registro y gestión adecuado de eventos (logs)	RIESGO 33 Error y/o fraude	8	7	56
No existe un documento de políticas, procedimientos y controles formales de transferencia información que viaja a través del uso de todo tipo de medios de comunicación	RIESGO 35 Incumplimiento	7	8	56

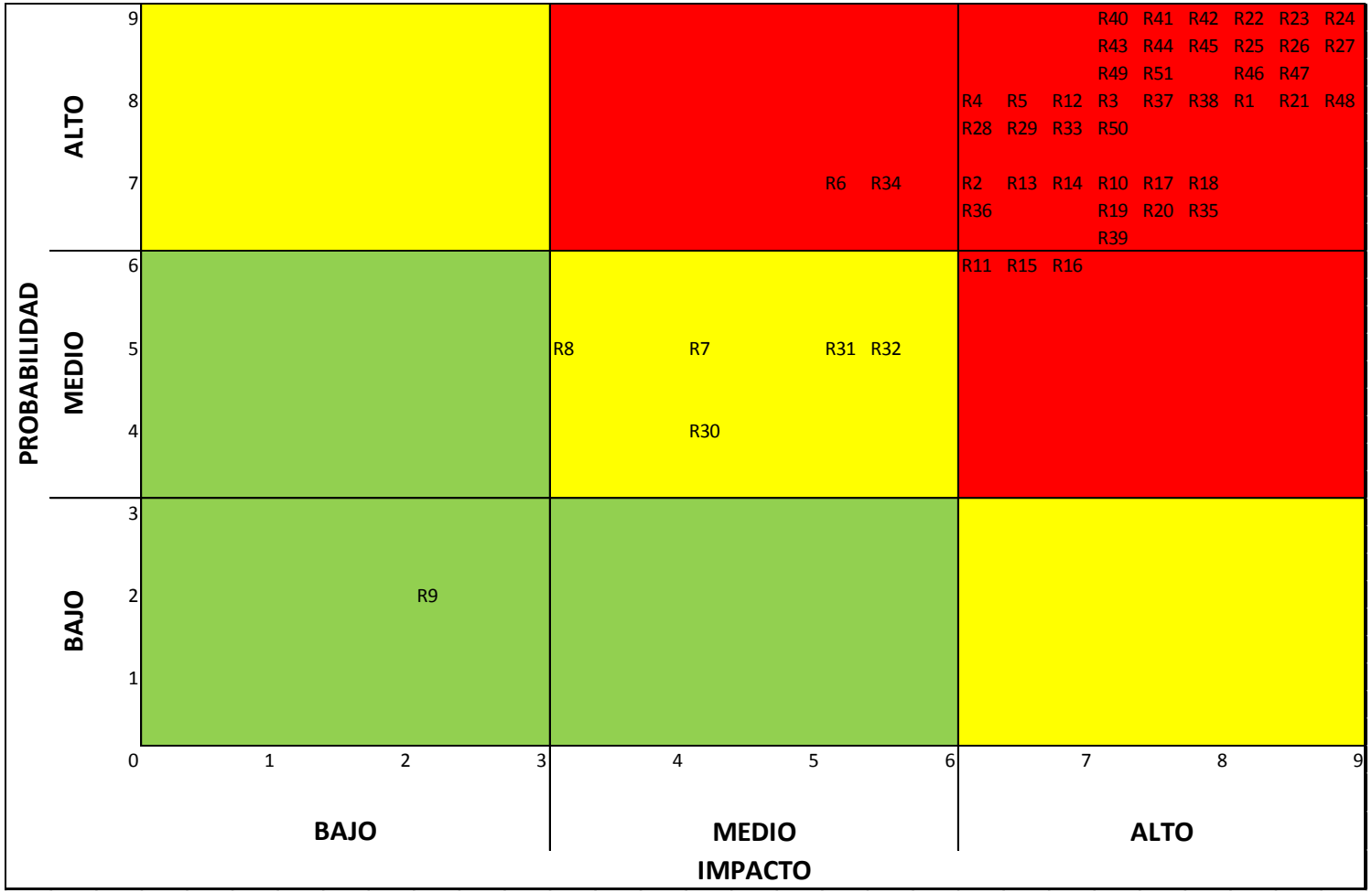
Los acuerdos con los proveedores no incluyen los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones	RIESGO 39 Incumplimiento	7	8	56
No existe la asignación de un responsable de seguridad de la información dentro del departamento de sistemas	RIESGO 2 Incumplimiento	7	7	49
No existen políticas y un proceso formal disciplinario de seguridad de la información comunicado a empleados, y monitoreo de cumplimiento	RIESGO 13 Incumplimiento	7	7	49
Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste no están claramente definidas, comunicadas a empleado o contratista y asignadas efectivamente.	RIESGO 14 Error y/o Fraude	7	7	49
No existen acuerdos de intercambio de la información	RIESGO 36 Incumplimiento	7	7	49
No se tiene definido un comité donde traten la seguridad de la información	RIESGO 6 Error y/o Fraude	7	6	42
No se archivan controles de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes	RIESGO 11 Error y/o Fraude	6	7	42
No se aplica un desarrollo e implementación de procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la Unidad Educativa	RIESGO 15 Error y/o Fraude	6	7	42
No se aplica procedimientos para la gestión de los medios informáticos removibles acordes con el	RIESGO 16 Error y/o Fraude	6	7	42

esquema de clasificación adoptado por la Unidad Educativa.				
No se han planificado y acordado los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales	RIESGO 34 Incumplimiento	7	6	42
No se documentan y aprueban los procedimientos operativos.	RIESGO 31 Incumplimiento	5	6	30
No tienen un manejo adecuado de cambios que afectan a la seguridad de la información en la Unidad Educativa y procesos de negocio, las instalaciones y sistemas de procesamiento de información	RIESGO 32 Error y/o fraude	5	6	30
Al no existir un responsable específico de SI o el gobierno IT, tampoco se tiene contacto con expertos de SI	RIESGO 7 Error y/o Fraude	5	5	25
La SI en relación a la gestión de proyectos no presenta un documento escrito que respalde la protección de la información.	RIESGO 8 Incumplimiento	5	4	20
No existe una política de puesto de trabajo despejado y bloqueo de pantalla	RIESGO 30 Incumplimiento	4	5	20
La SI en relación al uso de recursos móviles no presenta un documento escrito que respalde la protección de la información.	RIESGO 9 Incumplimiento	2	3	6

Realizado por: La autora

Ilustración 10 Matriz de evaluación de riesgos

MATRIZ DE EVALUACIÓN DE RIESGOS



Realizado por: La autora

4.4 Evaluación de Controles

Tabla 19 Evaluación y calificación de riesgos

DESCRIPCIÓN	RIESGO	TIPO DE CONTROL	ACCIÓN
La Unidad Educativa no tiene un documento que determine las políticas de seguridad de la información	**RIESGO 1 Incumplimiento**	PREVENIR, PROTEGER	Redactar un documento para cada área financiero-contable y sistemas en el que se detalle las políticas de seguridad de la información, con la finalidad de dar a conocer a los encargados del mismo. Solicitar la correspondiente aprobación.
No existe la asignación de un responsable de seguridad de la información dentro del departamento de sistemas	**RIESGO 2 Incumplimiento**	PREVENIR, EVITAR	Debería haber un Responsable de Seguridad de la Información, con sus respectivas responsabilidades. Cuya persona debe concientizar al personal para el cumplimiento de las Políticas de SI y monitorear a que se cumplan. Mantener actualizado las Políticas de SI.

Las políticas para la seguridad de la información no están aprobadas por la dirección, publicadas, ni comunicadas a los empleados.	**RIESGO 3 Incumplimiento**	PREVENIR, PROTEGER	Dar a conocer de forma escrita y verbal el documento aprobado a las personas encargadas de las áreas respectivas
Las políticas para la seguridad de la información al no estar redactadas en un documento no pueden ser revisadas con regularidad, y buscar mejoras significativas para garantizar su idoneidad, adecuación y efectividad.	**RIESGO 4 Incumplimiento**	PREVENIR, PROTEGER	Redactar un documento para cada área financiero-contable y sistemas el cual deberá ser revisado regularmente.
No existe una clara definición y asignación de responsabilidades para seguridad de la información	**RIESGO 5 Error y/o Fraude**	PREVENIR, EVITAR	Asignar un responsable de seguridad de la información dentro del departamento de sistemas
No se tiene definido un comité donde traten la seguridad de la información	**RIESGO 6 Error y/o Fraude**	PREVENIR, EVITAR	Si bien es pequeña la Institución en cuanto a tecnología, es necesario que se tenga un "Comité" que supervise cada cierto tiempo el cumplimiento de las Políticas de SI. Puede ser este el Comité o Las Reuniones de la Alta dirección de la Institución en donde se dé un espacio para los temas de TI y SI.
Al no existir un responsable específico de SI o el gobierno IT, tampoco se tiene contacto con expertos de SI	**RIESGO 7 Error y/o Fraude**	PREVENIR, EVITAR	El personal responsable de SI deberá tener conocimiento y dominar la ISO 27002

La SI en relación a la gestión de proyectos no presenta un documento escrito que respalde la protección de la información.	**RIESGO 8 Incumplimiento**	PREVENIR, PROTEGER	La SI en relación a la gestión de proyectos presenta un riesgo medio debido a que no presenta un documento escrito que respalde la protección de la información.
La SI en relación al uso de recursos móviles no presenta un documento escrito que respalde la protección de la información.	**RIESGO 9 Incumplimiento**	PREVENIR, PROTEGER	La SI en relación al uso de recursos móviles presenta un riesgo bajo debido a que no presenta un documento escrito que respalde la protección de la información.
No se ha implementado una política y medidas de seguridad de apoyo para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas al teletrabajo	**RIESGO 10 Incumplimiento**	PREVENIR, PROTEGER	Redactar un documento que se oriente a todos los departamentos de la Unidad Educativa en el que se detalle las políticas de seguridad de la información, con la finalidad de dar a conocer a los encargados del mismo.
No se archivan controles de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes	**RIESGO 11 Error y/o Fraude**	PREVENIR, PROTEGER	Debería haber una verificación de antecedentes de personal q ingresa y este en concordancia con regulaciones, ética y leyes relevantes
Todos los empleados de la Unidad Educativa, contratistas y usuarios de terceros no reciben entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales y de seguridad de la información relevantes para la función de su trabajo	**RIESGO 12 Error y/o Fraude**	PREVENIR, REDUCIR	Debería periódicamente, al menos una vez al año el personal de la Institución recibir un "entrenamiento" o recordatorio de las Políticas, Procesos y Procedimientos de SI para que cumplan las mismas.

No existen políticas y un proceso formal disciplinario de seguridad de la información comunicado a empleados, y monitoreo de cumplimiento	**RIESGO 13 Incumplimiento**	PREVENIR, PROTEGER	Luego de la definición de las Políticas de SI, se debe definir procesos y procedimientos básicos de SI. Las mismas se deben aprobar por la alta dirección y dar a conocer a todo el personal relacionado.
Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste no están claramente definidas, comunicadas a empleado o contratista y asignadas efectivamente.	**RIESGO 14 Error y/o Fraude**	PREVENIR, REDUCIR	Implementar una política, proceso y procedimiento de SI para el caso de empleados que finalizan y/o se cambian de puesto.
No se aplica un desarrollo e implementación de procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la Unidad Educativa	**RIESGO 15 Error y/o Fraude**	PREVENIR, PROTEGER	Si bien se manifiesta que se cuenta con responsables de activos de información, así como que se encuentran clasificados por su sensibilidad y criticidad. Se recomienda se haga nuevamente esta asignación y de clasificación y se tenga políticas, procesos y procedimientos de SI para el tratamiento de los mismos.
No se aplica procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la Unidad Educativa.	**RIESGO 16 Error y/o Fraude**	PREVENIR, PROTEGER	Implementar procedimientos para la gestión de los medios informáticos removibles.

No se han establecido, documentado, revisado y aprobado una política de control de accesos en base a las necesidades de seguridad y de negocio de la Unidad Educativa	**RIESGO 17 Incumplimiento**	PREVENIR, PROTEGER	Redactar un documento que se oriente a todos los departamentos de la Unidad Educativa en el que se detalle las políticas de control de accesos de SI.
No se existe un procedimiento formal de altas y bajas de usuarios con objeto de habilitar la asignación de derechos de acceso.	**RIESGO 18 Incumplimiento**	PREVENIR, PROTEGER	Redactar un documento que se oriente a todos los departamentos de la Unidad Educativa en el que se detalle las políticas de asignación de derechos de acceso.
No se ha implementado un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios	**RIESGO 19 Incumplimiento**	PREVENIR, PROTEGER	Redactar un documento que se oriente a todos los departamentos de la Unidad Educativa en el que se detalle un proceso formal de aprovisionamiento de accesos a los usuarios para todos los sistemas. Aplicar restricciones tanto para hardware como software para todos los usuarios.
No se exige a los usuarios el uso de las buenas prácticas de seguridad en el uso de información confidencial para la autenticación	**RIESGO 20 Error y/o Fraude**	PREVENIR, PROTEGER	Capacitar a los padres de familia y personal para las buenas prácticas de seguridad de la información
No tienen un manejo adecuado de gestión de contraseñas de usuario	**RIESGO 21 Error y/o Fraude**	PREVENIR, PROTEGER	Para ser almacenadas las contraseñas deben ser encriptadas

No se ha desarrollado e implementado una política que regule el uso de controles criptográficos (cifrado) para la protección de la información	**RIESGO 22 Incumplimiento**	PREVENIR, PROTEGER	Desarrollar e implementar una política que regule el uso de controles criptográficos
No se ha desarrollado e implementado una política de gestión de claves criptográficas a través de todo su ciclo de vida	**RIESGO 23 Incumplimiento**	PREVENIR, PROTEGER	Desarrollar e implementar una política de gestión de claves criptográficas
No se ha diseñado y aplicado un sistema de seguridad física a las oficinas, salas e instalaciones de los departamentos contable-financiero y sistemas	**RIESGO 24 Deterioro**	PREVENIR, PROTEGER, REDUCIR	Diseñar un sistema de seguridad física en las instalaciones de la Unidad Educativa
No se ha diseñado y aplicado una protección física/lógica contra desastres naturales, ataques maliciosos o accidentes	**RIESGO 25 Deterioro**	PREVENIR, PROTEGER, REDUCIR	Diseñar y aplicar una protección física contra desastres
No se ha diseñado y aplicado procedimientos para el desarrollo de trabajos y actividades en áreas seguras	**RIESGO 26 Incumplimiento**		Diseñar y aplicar procedimientos de seguridad física

Los equipos no se han reemplazado y protegido para reducir los riesgos de las amenazas y peligros ambientales	**RIESGO 27 Deterioro**	PREVENIR, PROTEGER, REDUCIR	Diseñar y aplicar una protección física contra desastres
Falta diseñar una infraestructura adecuada para que los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se encuentren protegidos contra la intercepción, interferencia o posibles daños	**RIESGO 28 Deterioro**	PREVENIR, PROTEGER, REDUCIR	Diseñar y aplicar una infraestructura adecuada
Falta actualizar la bitácora para que los equipos se mantengan adecuadamente y poder garantizar su disponibilidad e integridad continua.	**RIESGO 29 Deterioro**	PREVENIR, PROTEGER	Actualizar la bitácora
No existe una política de puesto de trabajo despejado y bloqueo de pantalla	**RIESGO 30 Incumplimiento**	PREVENIR, PROTEGER	Implementar políticas de trabajo despejado y bloqueo de pantalla
No se documentan y aprueban los procedimientos operativos.	**RIESGO 31 Incumplimiento**	PREVENIR, PROTEGER	Poner a disposición de los usuarios documentos de procedimientos operativos aprobados
No tienen un manejo adecuado de cambios que afectan a la seguridad de la información en la Unidad Educativa	**RIESGO 32 Error y/o fraude**	PREVENIR, PROTEGER	Tener un control adecuado de los cambios que afectan a la SI

y procesos de negocio, las instalaciones y sistemas de procesamiento de información			
No se maneja un registro y gestión adecuado de eventos (logs)	**RIESGO 33 Error y/o fraude**	PREVENIR, PROTEGER	Controlar un registro y gestión de eventos
No se han planificado y acordado los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales	**RIESGO 34 Incumplimiento**	PREVENIR, EVITAR	Involucrar la verificación de los sistemas operativos dentro de las actividades de auditoría
No existe un documento de políticas, procedimientos y controles formales de transferencia información que viaja a través del uso de todo tipo de medios de comunicación	**RIESGO 35 Incumplimiento**	PREVENIR, PROTEGER	Redactar un documento de políticas, procedimientos y controles del uso de todo tipo de medios de comunicación
No existen acuerdos de intercambio de la información	**RIESGO 36 Incumplimiento**	PREVENIR, PROTEGER	Redactar un documento de intercambio de información
No se identifica, revisa y documenta de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la Unidad Educativa para la protección de información	**RIESGO 37 Error y/o fraude**	PREVENIR, PROTEGER	Mientras no exista un documento de políticas, no se puede revisar de manera regular

No existen políticas de seguridad para las actividades de desarrollo del sistema que se hayan externalizado y se supervisa su cumplimiento	**RIESGO 38 Incumplimiento**	PREVENIR, EVITAR	Documentar políticas de seguridad para los sistemas externalizados, en el caso del Departamento financiero - contable con el programa SINET
Los acuerdos con los proveedores no incluyen los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones	**RIESGO 39 Incumplimiento**	PREVENIR, PROTEGER	Desarrollar y aplicar requisitos para abordar los riesgos con los proveedores
El departamento de sistemas no monitorea, revisa y audita la presentación de servicios del proveedor	**RIESGO 40 Error y/o fraude**	PREVENIR, PROTEGER	Monitorear, revisar y auditar los servicios realizados por el proveedor
No se administran los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos	**RIESGO 41 Incumplimiento**	PREVENIR, PROTEGER	Administrar cambios realizados por los proveedores
No se evalúa los eventos de seguridad de la información y se decide su clasificación como incidentes	**RIESGO 42 Error y/o fraude**	PREVENIR, PROTEGER	Desarrollar un documento de eventos de SI

No se tiene definido políticas y procedimientos de respuesta ante los incidentes de seguridad de la información en atención a los procedimientos documentados	**RIESGO 43 Incumplimiento**	PREVENIR, PROTEGER	Definir políticas y procedimientos de respuesta ante los incidentes de seguridad de la información
No se utiliza el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro	**RIESGO 44 Incumplimiento**	REDUCIR	Actualizar la bitácora
El departamento no define y aplica los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia	**RIESGO 45 Incumplimiento**	PREVENIR, PROTEGER	Implementar un respaldo de logs
La Unidad Educativa no ha determinado los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre	**RIESGO 46 Deterioro**	PREVENIR, PROTEGER, REDUCIR	Determinar los requisitos de seguridad para situaciones de crisis o desastre
La Unidad Educativa no establece, documenta, implementa, ni mantiene los procesos, procedimientos y controles para garantizar el mantenimiento del nivel	**RIESGO 47 Deterioro**	PREVENIR, PROTEGER, REDUCIR	Documentar los niveles necesarios de SI ante situaciones adversas

necesario de seguridad de la información durante situaciones adversas			
No se han identificado, documentado, ni se mantienen actualizados y de manera explícita para cada sistema de información y para la Unidad Educativa todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la Unidad Educativa para cumplir con estos requisitos	**RIESGO 48 Incumplimiento**	PREVENIR, PROTEGER	Redactar requisitos estatutarios, normativos y contractuales legislativos para cada sistema de información
No se utilizan controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas	**RIESGO 49 Error y/o fraude**	PREVENIR, PROTEGER	Implementar control de cifrado de la información
Por falta de documentación los jefes de área no pueden revisar regularmente el cumplimiento de políticas y procedimientos de seguridad de la información dentro de su área de responsabilidad.	**RIESGO 50 Incumplimiento**	PREVENIR, PROTEGER	Controlar la documentación respectiva
Al no existir un responsable de la SI no existe una revisión y comprobación de las políticas y	**RIESGO 51 Error y/o fraude**	PREVENIR, EVITAR	Al no existir un responsable de la SI no existe la revisión y comprobación de la mismas

procedimientos de seguridad de la información a nivel Organizacional			

Realizado por: La autora

4.5 Informe de auditoría

4.5.1 Carta de presentación del informe

Cuenca, 6 de octubre de 2017

OFICIO #2

ASUNTO: CARTA DE PRESENTACIÓN DEL INFORME

Ing.

Eleana Bojorque

Unidad Educativa “La Asunción”

Ciudad.

De mis consideraciones:

Se ha realizado la auditoría informática al sistema contable de la Unidad Educativa para el período 2017, empleando una planificación previa y posteriormente la ejecución de cada una de sus fases, con la finalidad de obtener un informe final de auditoría con resultados razonables. La información has sido obtenida exclusivamente de los departamentos contable-financiero y de sistemas.

Espero que los resultados expresados en el presente informe puedan ser considerados para optimizar y mejorar la seguridad informática del sistema contable.

Atentamente,

Denisse Uyaguari Ch.

4.5.2 Informe final de auditoría

Cuenca, 10 de octubre de 2017

Ing.

Eleana Bojorque

Unidad Educativa “La Asunción”

Ciudad.

De mis consideraciones:

Me dirijo de la manera más comedida a Ud. con la finalidad de poner en conocimiento el Informe Final de Auditoría Informática realizado al sistema contable de la Unidad Educativa referente al período 2017.

ENFOQUE DE LA AUDITORÍA

Fecha de inicio de auditoría:

28 de mayo de 2017

Fecha de redacción del Informe final de Auditoría:

6 de octubre de 2017

Equipo auditor:

Denisse Uyaguari

Alcance de auditoría:

Realizar una auditoría informática al sistema contable de la Unidad Educativa para el período 2017, basado en la norma ISO 27002 – Controles de Seguridad y elaboración de un informe con los resultados obtenidos.

Objetivos de la auditoría:

Objetivo general:

- Auditar la seguridad informática al sistema contable de la unidad educativa La Asunción, para el período 2017.

Objetivos Específicos

- Investigar el ambiente relacionado con la seguridad informática del sistema contable en la unidad educativa.
- Estudiar las buenas prácticas de gestión de seguridad de la información basado en la Norma ISO 27002.
- Elaborar un plan de auditoría.
- Ejecutar la auditoría y emitir un informe, detallando los resultados de la misma, incluyendo las observaciones y sus respectivas recomendaciones.

Componentes auditados:

- Departamento contable-financiero
- Departamento de Sistemas

INFORMACIÓN DE LA ENTIDAD

Misión:

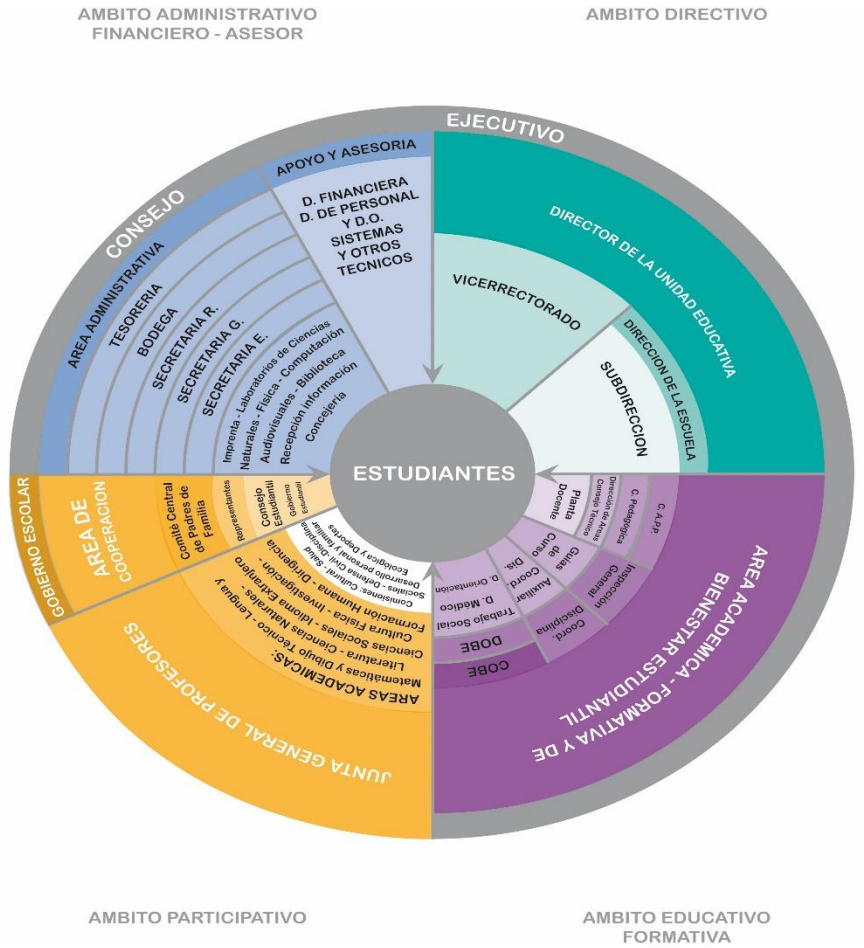
"Somos una Unidad Educativa Particular en mejora continua, conformada por profesionales en constante actualización, que brinda a niños y jóvenes un servicio educativo humanístico–integral, acorde con las últimas tendencias pedagógicas, científicas y tecnológicas, en un ambiente de calidez, compromiso y responsabilidad social." (Unidad Educativa La Asuncion, 2017)

Visión:

"Consolidarnos como Unidad Educativa de confianza y reconocimiento social, que se mantenga a la vanguardia de la educación, con propuestas pedagógicas innovadoras, ofreciendo una formación de seres humanos íntegros, que contribuyan a su transformación personal y del entorno social y ambiental." (Unidad Educativa La Asunción , 2017)

Estructura organizacional:

A continuación, se presenta la estructura organizacional de la Unidad Educativa La Asunción:



RESULTADOS GENERALES:

Observación:

- La Unidad Educativa no tiene un documento que determine las políticas de seguridad de la información.
- La SI en relación a la gestión de proyectos no presenta un documento escrito que respalde la protección de la información
- La SI en relación al uso de recursos móviles no presenta un documento escrito que respalde la protección de la información

- No se ha implementado una política y medidas de seguridad de apoyo para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas al teletrabajo
- No se han establecido, documentado, revisado y aprobado una política de control de accesos en base a las necesidades de seguridad y de negocio de la Unidad Educativa
- No se ha implementado un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios
- No se documentan y aprueban los procedimientos operativos.
- No existe un documento de políticas, procedimientos y controles formales de transferencia información que viaja a través del uso de todo tipo de medios de comunicación
- No existen políticas de seguridad para las actividades de desarrollo del sistema que se hayan externalizado y se supervisa su cumplimiento

Riesgo:

No se puede considerar que las políticas de seguridad de la información sean dadas a conocer únicamente de forma verbal, debido a que si existiera una negligencia o eventualidad por parte del departamento contable-financiero o de sistemas no existe la correspondiente documentación que respalde que las acciones están en contra de alguna política.

Recomendación #1:

Elaborar un documento que permita conocer las políticas y procedimientos a seguir referente a la seguridad de la información, el mismo que debe ser aprobado por la alta dirección, dar a conocer al personal correspondiente, regirse a su cumplimiento y ser revisadas con regularidad.

Redactar un documento que se oriente a todos los departamentos de la Unidad Educativa en el que se detalle un proceso formal de aprovisionamiento de accesos a los usuarios para todos los sistemas. Aplicar restricciones tanto para hardware como software para todos los usuarios

Documentar políticas de seguridad para los sistemas externalizados, en el caso del Departamento financiero - contable con el programa SINET

Observación:

No existe la asignación de un responsable de seguridad de la información dentro del departamento de sistemas.

Riesgo:

Al no existir la asignación de un responsable de seguridad de la información que pueda dirigir y controlar el cumplimiento de las actividades desempeñadas por el resto del personal del departamento, pueden ocurrir graves errores y/o fraudes con accesos libre a la información del sistema contable de la Unidad Educativa.

Recomendación #2:

Asignar un responsable de seguridad de la información, que tenga conocimiento de la ISO 27002, el mismo que pueda dirigir, revisar con regularidad, buscar mejoras significativas y monitorear el cumplimiento de las políticas y procedimientos de seguridad de la información a nivel organizacional.

Observación:

Todos los empleados de la Unidad Educativa, contratistas y usuarios de terceros no reciben entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales y de seguridad de la información relevantes para la función de su trabajo.

Riesgo:

Al no recibir un entrenamiento y actualizaciones adecuadas, los empleados pueden ejecutar acciones que para su criterio personal resulten ser las adecuadas, pero no se encuentren actualizadas, ni permitan la optimización de la seguridad informática.

Recomendación #3:

Organizar capacitaciones que se den a conocer las actualizaciones de las políticas, procedimientos organizacionales y seguridad de la información con la finalidad de que se ejecute de manera eficiente y eficaz las actividades en el trabajo desempeñado.

Observación:

- No se aplica un desarrollo e implementación de procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la Unidad Educativa
- No se aplica procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la Unidad Educativa.

Riesgo:

Al no tener procedimientos que determinen la manipulación de activos y gestión de los medios informáticos removibles, existe la probabilidad de que cualquier empleado pueda trasferir información confidencial por medio de ellos.

Recomendación #4:

Determinar por escrito los procedimientos adecuados para la manipulación de activos y gestión de medios informáticos removibles.

Observación:

- No se ha desarrollado e implementado una política que regule el uso de controles criptográficos (cifrado) para la protección de la información
- No se ha desarrollado e implementado una política de gestión de claves criptográficas a través de todo su ciclo de vida

Riesgo:

La inexistencia de políticas que regulen el uso y gestión de cifrado, provoca un manejo inadecuado de gestión de contraseñas de usuario, libre acceso perdiendo la autenticidad del origen de la información y siendo vulnerable el sistema a posibles modificaciones, hurto, sabotaje, falsificación, alteraciones, hackers, adulteración, etc.

Recomendación #5:

Desarrollar e implementar una política que regule el uso y gestión de controles y claves criptográficos

Observación:

- No se ha diseñado y aplicado un sistema de seguridad física a las oficinas, salas e instalaciones de los departamentos contable-financiero y de sistemas
- No se ha diseñado y aplicado una protección física/lógica contra desastres naturales, ataques maliciosos o accidentes
- No se ha diseñado y aplicado procedimientos para el desarrollo de trabajos y actividades en áreas seguras
- Los equipos no se han reemplazado y protegido para reducir los riesgos de las amenazas y peligros ambientales
- Falta diseñar una infraestructura adecuada para que los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se encuentren protegidos contra la intercepción, interferencia o posibles daños

Riesgo:

Al no existir un sistema de seguridad física a las oficinas e instalaciones del departamento contable-financiero y de sistemas, procedimientos de protección física contra desastres naturales o accidente y la infraestructura adecuada para proteger posibles daños, la información se puede perder en su totalidad y no existen respaldos de la base de datos a pesar de que existe un servidor, pero no cuenta lamentablemente con seguridad contra desastres.

Recomendación #6:

Establecer políticas y el debido protocolo a seguir en caso de desastres naturales, diseñar una infraestructura adecuada y aplicar procedimientos de seguridad física que respalden la seguridad de la información.

Observación:

No se identifica, revisa y documenta de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la Unidad Educativa para la protección de información

Riesgo:

La carencia de documentación de acuerdos de confidencialidad, origina que los empleados puedan divulgar y difundir la información porque no se encuentran comprometidos a mantener la confiabilidad y protección de la misma.

Recomendación #7

Elaborar la documentación con las respectivas legislaciones y acuerdos de confidencialidad e integridad de la información.

Observación:

- Los acuerdos con los proveedores no incluyen los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones
- El departamento de sistemas no monitorea, revisa y audita la presentación de servicios del proveedor

Riesgo:

La inexistencia de acuerdos, falta de monitoreo, revisión y auditoría a los servicios que presenta el proveedor al departamento contable-financiero, incide en que se pueda infringir errores o fraude que repercutan en la ejecución del programa contable.

Recomendación #8:

Definir acuerdos y actualizar contratos con los proveedores, que represente para ellos el compromiso de respaldar la seguridad de la información y ser monitoreados y auditados en base a las políticas establecidas.

Observación:

- Falta actualizar la bitácora para que los equipos se mantengan adecuadamente y poder garantizar su disponibilidad e integridad continua
- No se utiliza el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro

Riesgo:

Sin el respaldo de bitácoras, el administrador pasaría inadvertidos los eventos que ocurren en el sistema operativo.

Recomendación #9:

Mantener una buena administración y actualización de las bitácoras, conociendo el propósito de cada una de ellas, el formato en que se presenta la información y los ataques propios de cada servicio.

Observación:

- No se maneja un registro y gestión adecuado de eventos (logs)
- El departamento no define y aplica los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.

Riesgo:

La ausencia de la gestión de eventos produce que la detección de las tendencias y patrones fuera de lo común, resulte más complicados y que no se pueda tomar medidas defensivas de forma inmediata.

Recomendación #10:

Implementar un respaldo, controlar un registro y gestión de eventos

4.5.3 Convocatoria a la lectura del informe de auditoría.

Cuenca, 10 de octubre del 2017

Ing.

Eleana Bojorque

Unidad Educativa “La Asunción”

Ciudad.

De mis consideraciones:

Convoco a ustedes a una conferencia final de comunicación de resultados de la Auditoría Informática al Sistema Contable de la Unidad Educativa La Asunción, para el periodo 2017. La misma que se llevará a cabo en el rectorado de la unidad educativa, el día 12 de octubre del año 2017 a las 11h00.

Atentamente,

Denisse Uyaguari Ch.

4.6 Conclusiones y recomendaciones

4.6.1 Conclusiones

- La inexistencia de un documento que respalde las políticas y procedimientos de seguridad de la información dentro de la Unidad Educativa, expone a la misma a la manipulación de la información, al incumplimiento de legislaciones, normas y leyes, y ausencia de revisión o monitoreo de su cumplimiento.
- La falta de asignación de un responsable de SI, muestra la ausencia de mejoras y revisión continuas, así como la actualización y optimización en los procedimientos de seguridad de la información.
- No existe capacitaciones que permitan entrenar y actualizar a los empleados con expertos de SI.
- Ausencia de políticas y procedimientos a seguir en caso de eventualidades y siniestros.
- Ausencia de políticas que regule las claves criptográficas y cifrado.
- La inexistencia de un documento que respalde la confidencialidad e integridad de la información dentro de la Unidad Educativa, expone a la divulgación y trasferencia de la misma.
- La Unidad Educativa no ofrece una administración idónea y actualización de las bitácoras, ni un registro de logs.

4.6.2 Recomendaciones

- Elaborar un documento que permita conocer las políticas y procedimientos a seguir referente a la seguridad de la información, el mismo que debe ser aprobado por la alta dirección, dar a conocer al personal correspondiente, regirse a su cumplimiento y ser revisadas con regularidad.
- Redactar un documento que se oriente a todos los departamentos de la Unidad Educativa en el que se detalle un proceso formal de aprovisionamiento de accesos a los usuarios para todos los sistemas. Aplicar restricciones tanto para hardware como software para todos los usuarios
- Documentar políticas de seguridad para los sistemas externalizados, en el caso del Departamento financiero - contable con el programa SINET
- Asignar un responsable de seguridad de la información, que tenga conocimiento de la ISO 27002, el mismo que pueda dirigir, revisar con regularidad, buscar mejoras significativas y monitorear el cumplimiento de las políticas y procedimientos de seguridad de la información a nivel organizacional
- Organizar capacitaciones que se den a conocer las actualizaciones de las políticas, procedimientos organizacionales y seguridad de la información con la finalidad de que se ejecute de manera eficiente y eficaz las actividades en el trabajo desempeñado.
- Determinar por escrito los procedimientos adecuados para la manipulación de activos y gestión de medios informáticos removibles.
- Desarrollar e implementar una política que regule el uso y gestión de controles y claves criptográficos
- Establecer políticas y el debido protocolo a seguir en caso de desastres naturales, diseñar una infraestructura adecuada y aplicar procedimientos de seguridad física que respalden la seguridad de la información.
- Elaborar la documentación con las respectivas legislaciones y acuerdos de confidencialidad e integridad de la información
- Definir acuerdos y actualizar contratos con los proveedores, que represente para ellos el compromiso de respaldar la seguridad de la información y ser monitoreados y auditados en base a las políticas establecidas.

- Mantener una buena administración y actualización de las bitácoras, conociendo el propósito de cada una de ellas, el formato en que se presenta la información y los ataques propios de cada servicio.
- Implementar un respaldo, controlar un registro y gestión de eventos

Glosario

Backup	Copia de seguridad
Cifrado	Método escrito en letras, símbolos o números que seguridad a los archivos y mensajes
Encriptación	Codificación que convierte ilegible la información
Logs	Conocido también como logger o registrador de todos los eventos o acciones que afectan a un proceso particular.
SI	Seguridad de la Información
SINET	Sus siglas son definidas como: Solución Integral de Equipos Tecnológicos. Es el nombre del programa contable adquirido por la Unidad Educativa La Asunción

Bibliografía

GESCONSULTOR. (10 de 2013). *ISO27002.es*. Obtenido de El portal de ISO 27002 en Español: http://iso27000.es/iso27002.html

José, Z. (Septiembre de 2012). Proyecto Educativo Institucional. *Organigrama Institucional*. Cuenca, Azuay, Ecuador.

Richard, R. (18 de 08 de 2016). *Romero Richard*. Obtenido de Norma ISO 17799: http://estratega.org/todo-lo-que-ud-debe-saber-de-la-norma-de-seguridad-iso-17-799/

SGSI. (14 de 08 de 2013). *SGSI*. Obtenido de Blog especializado en Sistemas de Gestión : http://www.pmg-ssi.com/2013/08/la-nch-iso-27001-origen-y-evolucion/

Unidad Educativa La Asunción . (16 de Septiembre de 2017). *Unidad Educativa La Asuncion*. Obtenido de Portaluea: http://www.laasuncion.edu.ec/portaluea/index.php/about-us/misi%C3%B3n-y-visi%C3%B3n

Unidad Educativa La Asuncion. (16 de Septiembre de 2017). *Unidad Educativa La Asuncion*. Obtenido de Portaluea: http://www.laasuncion.edu.ec/portaluea/index.php/about-us/misi%C3%B3n-y-visi%C3%B3n

Doctora Jenny Ríos Coello, Secretaria de la Facultad de Ciencias de la Administración de la Universidad del Azuay

C E R T I F I C A:

Que, el Consejo de Facultad en sesión del 17 de mayo de 2017, conoció la petición de la estudiante **DENISSE GABRIELA UYAGUARI CHALCO** con código **65915**, que presenta el diseño de su trabajo de titulación denominado: ***"AUDITORÍA DE SEGURIDAD INFORMÁTICA AL SISTEMA CONTABLE DE LA UNIDAD EDUCATIVA LA ASUNCIÓN, PARA EL PERÍODO 2017"***, presentado previa a la obtención del título de Ingeniera en Contabilidad y Auditoría.- El Consejo de Facultad acogió el informe de la Junta Académica de Contabilidad Superior y resolvió aprobar el diseño. Designa como **Director al ingeniero Pablo Pintado Zumba** y como miembros del Tribunal Examinador al ingeniero Diego Condo Daquilema y al ingeniero Juan Carlos Aguirre Maxi.- En esta misma sesión el Consejo de Facultad fija como plazo para la entrega del trabajo de titulación, seis meses contados desde la fecha de su aprobación, esto es hasta el **17 de Noviembre de 2017,** debiendo el Director presentar a la Junta Académica, dos informes bimensuales del desarrollo del trabajo de titulación.

Cuenca, 18 de mayo de 2017

Dra. Jenny Ríos Coello
Secretaria de la Facultad de
Ciencias de la Administración

UNIVERSIDAD DEL AZUAY
FACULTAD DE ADMINISTRACIÓN
SECRETARÍA

C O N V O C A T O R I A

Por disposición de la Junta Académica de **Contabilidad Superior**, se convoca a los Miembros del Tribunal Examinador, a la sustentación del Protocolo del Trabajo de Titulación: **"AUDITORIA DE SEGURIDAD INFORMÁTICA AL SISTEMA CONTABLE DE LA UNIDAD EDUCATIVA LA ASUNCIÓN, PARA EL PERÍODO 2017"**, presentado por la estudiante **Denisse Gabriela Uyaguari Chalco** con código **65915** previa a la obtención del grado de Ingeniera en Contabilidad y Auditoría, para el día **MARTES 25 DE ABRIL DE 2017 A LAS 09h00.**

Cuenca, 18 de abril de 2017

Dra. Jenny Ríos Coello
Secretaria de la Facultad

Ing. Pablo Pintado Zumba .....

Ing. Diego Condo Daquilema .....

Ing. Juan Carlos Aguirre Maxi .....

mjmr/

Recibido el 18-04-2017.

ACTA
SUSTENTACIÓN DE PROTOCOLO/DENUNCIA DEL TRABAJO DE TITULACIÓN

1.1 **Nombre del estudiante:** **Denisse Gabriela Uyaguari Chalco** con código **65915**
Director sugerido: Ing. Pablo Pintado Zumba
1.2 **Codirector (opcional):** _____
1.3 **Tribunal:** Ing. Diego Condo Daquilema/ Ing. Juan Carlos Aguirre Maxi
1.4 **Título propuesto:** **"AUDITORIA DE SEGURIDAD INFORMÁTICA AL SISTEMA CONTABLE DE LA UNIDAD EDUCATIVA LA ASUNCIÓN, PARA EL PERÍODO 2017"**
1.5 **Resolución:**

1.5.1 Aceptado sin modificaciones _____

1.5.2 Aceptado con las siguientes modificaciones:

_____

_____

_____

1.5.3 Responsable de dar seguimiento a las modificaciones: Ing. Pablo Pintado Zumba
1.5.4 No aceptado
- Justificación:

_____
_____
_____

Tribunal

.....	.....	.....
Ing. Pablo Pintado Zumba	Ing. Diego Condo Daquilema	Ing. Juan Carlos Aguirre Maxi

.....
Srta. Denisse Gabriela Uyaguari Chalco

Dra. Jenny Ríos Coello
Secretario de Facultad

Fecha de sustentación: día **MARTES 25 DE ABRIL DE 2017 A LAS 09h00**

RÚBRICA PARA LA EVALUACIÓN DEL PROTOCOLO DE TRABAJO DE TITULACIÓN

1.1 Nombre del estudiante: Denisse Gabriela Uyaguari Chalco
con código 65915
1.2 Director sugerido: Ing. Pablo Pintado Zumba
1.3 Codirector (opcional):
1.4 Título propuesto: **"AUDITORIA DE SEGURIDAD INFORMÁTICA AL SISTEMA CONTABLE DE LA UNIDAD EDUCATIVA LA ASUNCIÓN, PARA EL PERÍODO 2017"**
1.5 Revisores (tribunal): Ing. Diego Condo Daquilema/ Ing. Juan Carlos Aguirre Maxi
Recomendaciones generales de la revisión:

	Cumple totalmente	Cumple parcialmente	No cumple	Observaciones (*)
Línea de investigación				
1. ¿El contenido se enmarca en la línea de investigación seleccionada?	✓			
Título Propuesto				
2. ¿Es informativo?	✓			
3. ¿Es conciso?	✓			
Estado del arte				
4. ¿Identifica claramente el contexto histórico, científico, global y regional del tema del trabajo?	✓			
5. ¿Describe la teoría en la que se enmarca el trabajo	✓			
6. ¿Describe los trabajos relacionados más relevantes?	✓			
7. ¿Utiliza citas bibliográficas?	✓			
Problemática y/o pregunta de investigación				
8. ¿Presenta una descripción precisa y clara?	✓			
9. ¿Tiene relevancia profesional y social?	✓			
Hipótesis (opcional)				
10.¿Se expresa de forma clara?	✓			
11.¿Es factible de verificación?	✓			
Objetivo general				
12.¿Concuerda con el problema formulado?	✓			
13.¿Se encuentra redactado en tiempo verbal infinitivo?	✓			
Objetivos específicos				

14.¿Concuerdan con el objetivo general?	✓			
15.¿Son comprobables cualitativa o cuantitativamente?	✓			
Metodología				
16.¿Se encuentran disponibles los datos y materiales mencionados?	✓			
17.¿Las actividades se presentan siguiendo una secuencia lógica?	✓			
18.¿Las actividades permitirán la consecución de los objetivos específicos planteados?	✓			
19.¿Los datos, materiales y actividades mencionadas son adecuados para resolver el problema formulado?	✓			
Resultados esperados				
20.¿Son relevantes para resolver o contribuir con el problema formulado?	✓			
21.¿Concuerdan con los objetivos específicos?	✓			
22.¿Se detalla la forma de presentación de los resultados?	✓			
23.¿Los resultados esperados son consecuencia, en todos los casos, de las actividades mencionadas?	✓			
Supuestos y riesgos				
24.¿Se mencionan los supuestos y riesgos más relevantes?	✓			
25.¿Es conveniente llevar a cabo el trabajo dado los supuestos y riesgos mencionados?	✓			
Presupuesto				
26.¿El presupuesto es razonable?	✓			
27.¿Se consideran los rubros más relevantes?	✓			
Cronograma				
28.¿Los plazos para las actividades son realistas?	✓			
Referencias				
29.¿Se siguen las recomendaciones de normas internacionales para citar?	✓			
Expresión escrita				
30.¿La redacción es clara y fácilmente comprensible?	✓			
31.¿El texto se encuentra libre de faltas ortográficas?	✓			

(*) Breve justificación, explicación o recomendación.

- Opcional cuando cumple totalmente,
- Obligatorio cuando cumple parcialmente y NO cumple.

.....

.....

.....

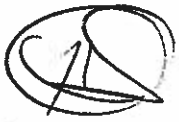
.....	.....	.....
Ing. Pablo Pintado Zumbà	Ing. Diego Condo Daquilema	Ing. Juan Carlos Aguirre Maxi

FECHA: 18-04-2017

ESCUELA DE CONTABILIDAD SUPERIOR

ESTUDIANTE: Denisse Gabriela Uyaguari Chalco.

Procede Trabajo Titulación



Martes, 25 abril 2017
09h00

Pablo Pintado
Diego Condo
Juan Carlos Aguirre.

UNIVERSIDAD DEL AZUAY
FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
DIRECCIÓN ESCUELA DE CONTABILIDAD SUPERIOR

OFICIO: No. 0109-2017-ECS
ASUNTO: Conocimiento de propuesta de Trabajo de Titulación
FECHA: Cuenca, 11 de abril de 2017.

Señor Ingeniero
Oswaldo Merchán Manzano
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
En su despacho:

Señor Decano:

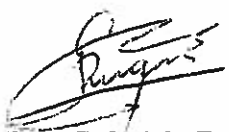
La Junta Académica de la Escuela de Contabilidad Superior, reunida el día 11 de abril del año en curso, conoció la propuesta del proyecto de trabajo de titulación, denominado: "Auditoría de seguridad informática al sistema contable de la Unidad Educativa La Asunción, para el periodo 2017", presentado por la señorita Uyaguari Chalco Denisse Gabriela, con código No. 65915, estudiante de la Carrera de Contabilidad Superior, previo a la obtención del título de Ingeniera en Contabilidad y Auditoría.

A fin de aplicar la guía de elaboración y presentación de la denuncia/protocolo de trabajo de titulación, la Junta Académica de la Carrera de Contabilidad Superior, considera que la propuesta presentada por la estudiante, debe ser analizada y evaluada por el Tribunal que estará integrado por: Ing. Pablo Pintado Zumba, como Director, y como miembros del tribunal al Ing. Diego Condo Daquilema, y al Ing. Juan Carlos Aguirre Maxi, quienes deberán verificar que el diseño contenga una estructura teórica, metodológica, técnica, objetiva y coherente, y cumpla con los requisitos establecidos en la guía antes mencionada. El Tribunal designado recibirá la sustentación del diseño del Trabajo de Titulación, previo al desarrollo del mismo.

En caso de existir la aprobación con modificaciones la Junta Académica resuelve que el Ing. Pablo Pintado Zumba, Director del diseño sea quién realice el seguimiento a las modificaciones recomendadas.

Por lo expuesto solicitamos se realice el trámite correspondiente, y el tribunal suscriba el acta de sustentación de la denuncia del trabajo de titulación.

Atentamente,



Ing. Gabriela Duque Espinoza
Coordinadora de la Carrera de Contabilidad Superior

UNIVERSIDAD DEL AZUAY

Cuenca, 11 de abril de 2017

Ingeniero
Oswaldo Merchán Manzano
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
Su despacho.

De mi consideración:

Reciba un cordial saludo, por medio de la presente yo Denisse Gabriela Uyaguari Chalco, con código 65915 estudiante de la escuela de Contabilidad Superior de la Facultad de Ciencias de la Administración, solicito a Ud. me apruebe el diseño de mi trabajo de titulación con el tema "AUDITORÍA DE SEGURIDAD INFORMÁTICA AL SISTEMA CONTABLE DE LA UNIDAD EDUCATIVA LA ASUNCIÓN, PARA EL PERÍODO 2017.", previo a la obtención del título de Ingeniero en Contabilidad y Auditoría.

En espera de una respuesta favorable a la presente, anticipo mis agradecimientos.

Atentamente:

Denisse Gabriela Uyaguari Chalco

Código:65915

UNIVERSIDAD DEL AZUAY

DOCTORA JENNY RIOS COELLO, SECRETARIA DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACION DE LA UNIVERSIDAD DEL AZUAY

C E R T I F I C A:

Que, la señorita **UYAGUARI CHALCO DENISSE GABRIELA** con código **65915** alumna de la escuela de **CONTABILIDAD SUPERIOR**, tiene aprobado más del 80% de los créditos de su malla de estudios.

Que, a la señorita **UYAGUARI CHALCO DENISSE GABRIELA** le falta aprobar las siguientes asignaturas para finalizar sus estudios:

COMERCIO EXTERIOR

AUDITORÍA DE CALIDAD

Cuenca, 04 de marzo de 2017

Derecho No. **001-002-000057160**

mjmr.

UNIV... AZUAY
FAC... DE
ADM... TRACION
SEC... TARIA

Edición autorizada de 10 000 ejemplares
Del 788 501 al 798 500
Nº 0791712

UNIDAD EDUCATIVA
LA ASUNCIÓN

Oficio N°/0099/SR/CA
Cuenca, 04 abril de 2017

Ingeniero
Oswaldo Merchán Manzano
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
Presente

De mi consideración

Mediante el presente, doy a conocer a usted, que la señorita DENISSE GABRIELA UYAGUARI CHALCO, estudiante del décimo ciclo de la Escuela de Contabilidad Superior de la Universidad del Azuay matriculada bajo el código 65915, cuenta con la autorización respectiva para realizar su Tesis de Grado con el título de "Auditoría de Seguridad Informática al Sistema Contable de la Unidad Educativa La Asunción durante el año 2017".

Por la favorable atención que se sirva dar a la presente.

Atentamente

UNIDAD EDUCATIVA PARTICULAR "LA ASUNCIÓN" RECTORADO CUENCA - ECUADOR

Dra. Patricia Arévalo S.
RECTORA (E) DE LA UNIDAD EDUCATIVA

PA/mst

PBX (593 7) 2816998 2880014
2885585 2884017 2883234

Cuenca, 06 de abril de 2017

Ingeniero
Oswaldo Merchán Manzano
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
UNIVERSIDAD DEL AZUAY

De mi consideración,

Yo, Ing. Pablo Pintado Zumba informo que he revisado el protocolo de trabajo de titulación elaborado por la estudiante Denisse Gabriela Uyaguari Chalco, con código estudiantil 65915, previo a la obtención del título de Ingeniera en Contabilidad y Auditoría, denominado "AUDITORÍA DE SEGURIDAD INFORMÁTICA AL SISTEMA CONTABLE DE LA UNIDAD EDUCATIVA LA ASUNCIÓN, PARA EL PERÍODO 2017", protocolo que a mi criterio, cumple con los lineamientos y requerimientos establecido por su carrera.

Por lo expuesto, me permito sugerir que sea considerado para la revisión y sustentación del mismo,

Sin otro particular, me suscribo,

Atentamente,

Ing. Pablo Pintado Zumba.

UNIVERSIDAD DEL AZUAY

UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN

ESCUELA DE CONTABILIDAD SUPERIOR

PROTOCOLO DE TRABAJO DE TITULACIÓN

TÍTULO: "AUDITORÍA DE SEGURIDAD INFORMÁTICA AL SISTEMA CONTABLE DE LA UNIDAD EDUCATIVA LA ASUNCIÓN, PARA EL PERÍODO 2017."

NOMBRE DEL ESTUDIANTE: Denisse Gabriela Uyaguari Chalco

DIRECTOR SUGERIDO: Ing. Pablo Fernando Pintado Zumba

CUENCA – ECUADOR

2017

UNIVERSIDAD DEL AZUAY

1. DATOS GENERALES

1.1 Nombre del estudiante: Uyaguari Chalco Denisse Gabriela.

1.1.1 Código: 65915

1.1.2 Contacto:

Teléfono: 2901181

Celular: 0987736501

Correo: dudis_uyaguari@hotmail.com

1.2 Director sugerido: Pintado Zumba Pablo Fernando, Magister en Administración de Empresas.

1.2.1 Contacto:

Celular: 0997031452

Correo: pablopintado@hotmail.com

1.3 Co-director sugerido:

1.3.1 Contacto:

1.4 Asesor metodológico:

1.5 Tribunal designado:

1.6 Aprobación:

1.7 Línea de Investigación de la carrera: 5311 Organización y Dirección de Empresas

1.7.1 Código UNESCO: 5311.02 Gestión Financiera y Auditoría

1.7.2 Tipo de trabajo:

a. Proyecto de Investigación.

b. Investigación Formativa.

1.8 Área de estudio:

- Contabilidad General I y II
- Informática I y II
- Administración estratégica y Gestión de Riesgos
- Auditoría de Sistemas y Tic
- Auditoría de Calidad

1.9 Título propuesto: "Auditoría de seguridad informática al sistema contable en la unidad educativa La Asunción, para el período 2017."

1.10 Subtitulo:

1.11 Estado del proyecto: Proyecto nuevo.

UNIVERSIDAD DEL AZUAY

2. CONTENIDO

2.1 Problemática:

Los sistemas informáticos deben estar manejados y basados comúnmente en pilares de seguridad de la información como la disponibilidad, confidencialidad, autenticidad e integridad, en los que se sustenta tanto las aplicaciones, actividades, acciones y herramientas que de él se desprenden. Se puede indicar específicamente que el sistema de contabilidad de la unidad educativa La Asunción, con sede en la ciudad de Cuenca, desde el año de 1963 que fue fundada hasta la actualidad no ha presentado una auditoría de seguridad informática al sistema contable, por ello queremos contar con evidencias que determinen el cumplimiento de los pilares antes mencionados.

2.2 Pregunta de investigación:

¿El sistema contable de la unidad educativa La Asunción cumple con las buenas prácticas de gestión de la seguridad de la información?

2.3 Resumen

Hoy en día muchas entidades públicas o privadas no cuentan con el asesoramiento adecuando sobre la seguridad informática al sistema contable; y se ven reflejadas en malas decisiones.

Este es el caso de la unidad educativa La Asunción, la cual no ha presentado una auditoría sobre la seguridad informática a su sistema contable. Es por ello que la tesis propuesta hace énfasis en la realización de un plan de auditoría y su aplicación práctica, que involucra grandes beneficios para la misma, en cuanto a la identificación y eliminación de debilidades y riesgos, mejorar las seguridades existentes y realizar nuevas propuestas. Para

su efecto, se basará en la norma ISO 27002 –Controles de Seguridad que recomienda abordar objetivos de control derivados de los riesgos para la confidencialidad, integridad y disponibilidad de información. La norma pretende también proporcionar una guía para el desarrollo de estándares de seguridad organizacional y prácticas de gestión de seguridad efectiva y ayudar a construir confianza en las actividades.

2.4 Estado del arte y marco teórico

Se debe tomar en cuenta que es importante llevar un control claro de los sistemas contables y las diferentes cuentas que se genera en la empresa para poder brindar un servicio claro y conciso a sus clientes, evitando que se genere pérdida para la misma, manteniendo un control de cada uno de los servicios que ofrece, generando orden en la unidad eductiva. Al no tener auditorías de seguridad informática al sistema contable de manera efectiva, genera una gran cantidad de problemas pues no se tiene un conocimiento exacto de las distintas actividades que influyen al elaborar y brindar un servicio. Existen varias amenazas que resultan perjudícales para la entidad, generando pérdidas cuantitativas de dinero que no se conoce con exactitud sus valores, ni los errores que provocaron dichas pérdidas. Falta de seguridad e integridad de los datos que respalden la confidencialidad de la información contable y financiera de la unidad educativa.

Según Santandreu (2009) plantea que "La empresa debe hacer aquello que la haga mejor que sus competidores" (p.196), señalando que debe enfocarse en aquellos problemas que dificultan llegar a competir con otras unidades educativas.

Adicionalmente, se debe tener en claro que la auditoría es un examen sistemático de los registros y las operaciones para determinar si están o no de acuerdo con los principios y las

normas establecidas. Teniendo por objetivo determinar la razonabilidad, integridad y autenticidad de los estados financieros, datos, expedientes y demás documentos contables presentados por la dirección.

Según lo planteado por Rivas (2009), "La auditoría informática es un examen metódico de un sistema informático en particular, realizado de una forma puntual, a instancias de la dirección, con la intención de ayudar a mejorar conceptos como la seguridad, la eficacia y la rentabilidad del sistema, que resultan auditados" (p. 39), por medio de este tipo de auditoria se podrá recoger , agrupar y evaluar evidencias para determinar si el sistema de información cumple con los pilares de seguridad informática como disponibilidad, confidencialidad, integridad y autenticidad.

Dentro de los lineamientos mencionados por Porto y Merino (2016) afirman que:

> La noción de sistema contable, de este modo, puede entenderse de distintas maneras. En su sentido más amplio, se trata del conjunto de elementos que registran la información financiera y las interrelaciones de estos datos. Esta estructura, por sus características, contribuye a la toma de decisiones en el ámbito de la gerencia. (p. 30)

Con la implementación de una auditoría al sistema contable se podrá medir, evaluar, y calificar sistemática y estructuralmente información cuantitativa y cualitativa basada en hechos económicos que realiza la unidad educativa, se tendrá control sobre cada una de sus transacciones, se podrá conocer la evolución económica día a día, se identificará ciertos eventos económicos que la afectan a la entidad directa e indirectamente y se tomará decisiones en base a los resultados obtenidos.

Entre las ventajas que proporciona una auditoría informática al sistema contable basado en las buenas prácticas de gestión de seguridad de la información se puede mencionar: seguridad en la información para que pueda ser accedida únicamente por las personas que tienen autorización para hacerlo, y no sea borrada, copiada o alterada, no sólo en su trayecto, sino también en su origen. Precaución contra posibles daños, tanto en la información como en el acceso a la misma: ataques o accidentes. Diseñar controles y medidas correctivas en la seguridad de la información.

La norma ISO 27002 que hace referencia a los controles de seguridad, será una guía para el desarrollo de 14 dominios que se consideran desde diferentes perspectivas para proteger la información por lo que también se introducen objetivos de control y controles muy específicos para el mantenimiento, desarrollo y adquisición de sistemas, medidas de seguridad para la relación con los proveedores, gestionar los incidentes de seguridad, la continuidad de negocio, entre otros.

De esta forma se tiene la certeza que al elaborar una auditoría de seguridad informática al sistema contable se llegará a determinar el cumplimiento de buenas prácticas de gestión de seguridad de la información de la unidad educativa, los riesgos y amenazas que afectan al buen funcionamiento, así también poder establecer controles y efectuar medidas correctivas que se apliquen en el sistema contable, generando un valor mucho más concreto y eficiente para los procesos y diferentes actividades que se van a llevar a cabo.

2.5 Hipótesis:

UNIVERSIDAD DEL AZUAY

2.6 Objetivo general:

- Auditar la seguridad informática al sistema contable de la unidad educativa La Asunción, para el período 2017.

2.7 Objetivos Específicos

- Investigar el ambiente relacionado con la seguridad informática del sistema contable en la unidad educativa.
- Estudiar las buenas prácticas de gestión de seguridad de la información basado en la Norma ISO 27002.
- Elaborar un plan de auditoria.
- Ejecutar la auditoría y emitir un informe, detallando los resultados de la misma, incluyendo las observaciones y sus respectivas recomendaciones.

2.8 Metodología

- Para el desarrollo de la presente investigación se utilizará el método analítico en la investigación del área contable de la unidad educativa La Asunción con sede en la ciudad de Cuenca; partiremos aplicando técnicas de verificación escrita y documental que se desarrollarán a través de la aplicación de un cuestionario de control interno dirigida al jefe del departamento contable- financiero para recopilar toda la información solicitada referente a las falencias o inconvenientes en la seguridad de la información del sistema contable. Se analizará el cumplimiento de las buenas prácticas de gestión de seguridad de la información basado en la norma ISO 27002. Se realizará un plan de

auditoría de seguridad de la información para el sistema contable de la unidad educativa. Finalmente, se ejecutará la auditoría y se dará a conocer mediante el informe respectivo las recomendaciones y conclusiones dirigida al jefe del departamento auditado.

2.9 Alcances y resultados esperados:

Como resultado a los objetivos específicos propuestos anteriormente se obtendrá un informe de auditoría basado en la Norma ISO 27002 – Controles de Seguridad y se podrá determinar controles o medidas preventivas, evaluar los riesgos informáticos, con el propósito de dar a conocer las falencias que se presentan en la unidad educativa y recomendar a los administradores los procedimientos que se deben llevar a cabo para salvaguardar la información que se maneja.

2.10 Supuestos y riesgos:

Ninguno

2.11 Presupuesto:

RUBRO/DENOMINACIÓN	COSTO USD	JUSTIFICACIÓN
Suministros de oficina	$20.00	Se adquirirá implementos como hojas, cuadernos, esferos y otros para el desarrollo de la investigación.
Impresiones	$20.00	Éstas serán para presentar los avances en caso de ser necesario y el trabajo final.

CD	$3.00	Se realizará una copia del trabajo final para la revisión por parte del tribunal.
Folders	$3.00	Servirá para presentar los avances y guardar los documentos adicionales de la investigación.
Anillado	$5.00	Su utilización será para presentar el trabajo final.
Movilización	$40.00	Incurren los gastos de transporte hacia y desde la empresa donde se realiza la investigación.
Copias	$20.00	Se entregaran a los miembros del tribunal y tutor.
Imprevistos	$50.00	Es un fondo para posibles gastos fortuitos.
TOTAL	**$161.00**	

2.12 Financiamiento:

El proyecto será financiado por la autora.

2.13 Esquema tentativo

Agradecimientos

Responsabilidad

Resumen

Abstract

Introducción

UNIVERSIDAD DEL AZUAY

4.3 Evaluación y calificación del riesgo

4.4 Evaluación de Controles

4.5 Informe de auditoría

4.6 Conclusiones y recomendaciones

Referencia Bibliográfica

Anexos

2.14 Cronograma

Objetivo Específico	Actividad	Resultado Esperado	Tiempo (Semana
1. Investigar el ambiente relacionado con la seguridad informática del sistema contable en la unidad educativa	1.1 Fundamentos generales	1.1.1 Introducción	8 semanas
		1.1.2 Historia	
		1.1.3 Misión	
		1.1.4 Estructura orgánico general	
		1.1.5 Estructura orgánico-funcional del departamento Contable-Financiero	
		1.1.6 Situación actual de la seguridad informática del sistema contable en	

		la unidad educativa.	
2. Estudiar las buenas prácticas de gestión de seguridad de la información basado en norma ISO 27002.	2.1 Buenas prácticas seguridad de la información.	2.1.1 Reseña histórica de la Norma ISO 17799 2.2.2 Generalidades de la Norma ISO 27002 – Controles de Seguridad	4 Semanas
3. Elaborar un plan de auditoría	3.1 Plan de auditoría para la gestión de seguridad de la información del sistema contable	3.1.1 Alcance. 3.1.2 Fuentes de información. 3.1.3 Cronograma de actividades. 3.1.4 Herramientas útiles para el desarrollo de la auditoría.	2 Semanas
4. Ejecutar la auditoría y emitir un informe, detallando los resultados de la misma, incluyendo las observaciones y sus respectivas recomendaciones.	4.1 Ejecución del plan de auditoría	4.1.1 Análisis de transacciones y recursos 4.1.2 Identificación de riesgos y amenazas 4.1.3 Evaluación y calificación del riesgo 4.1.4 Evaluación de Controles 4.1.5 Informe de auditoría	8 Semanas

UNIVERSIDAD DEL AZUAY

		4.1.6 Conclusiones y recomendaciones	
TOTAL			22

2.15 Referencias:

Bibliografía

El portal de ISO 27002 en Español. (s.f.). Obtenido de El portal de ISO 27002 en Español: http://www.iso27000.es/iso27002.html

Estado, C. G. (s.f.). *Contraloría General del Estado*. Obtenido de http://www.contraloria.gob.ec/LaInstitucion/CodigoEtica

Evelyn, Q. (2012). *slideshare*. Obtenido de http://es.slideshare.net/evelynquiroz14/auditora-informtica-en-los-procesos-contables

LOEPS, R. (2012). *OAS*. Obtenido de http://www.oas.org/juridico/PDFs/mesicic4_ecu_regla2.pdf

Margarita, C. O. (14 de noviembre de 2012). *Gestipolis*. Obtenido de http://www.gestiopolis.com/auditoria-de-sistemas-de-informacion/

Martínez, Y. A. (2012). *Redalyc*. Obtenido de http://www.redalyc.org/articulo.oa?id=193924743004

Merino, P. y. (2016). *Auditoría Informática.*

Rivas. (2009). *Auditoría informática.*

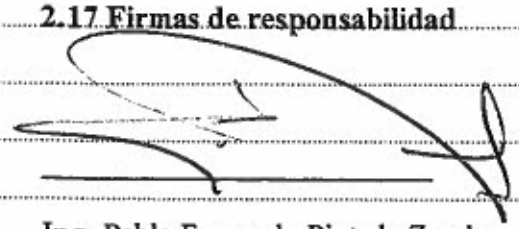
Santandreu. (2009). *Auditoría de Gestión.*

SENPLADES. (2009). *SENPLADES.* Obtenido de ppikas.files.wordpress: https://ppikas.files.wordpress.com/2009/06/senplades-instructivopoa.pdf

Sinnexus. (2009). *SInnexus.* Obtenido de Business Intelligence Informática estratégica: http://www.sinnexus.com

2.16 Anexos

2.17 Firmas de responsabilidad



Ing. Pablo Fernando Pintado Zumba

2.18 Firma de responsabilidad

Denisse Gabriela Uyaguari Chalco

2.19 Fecha de entrega