

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



CENTRO DE EDUCACION CONTINUA

"AUDITORIA EN EL PROCESO DE FACTURACION"

TESIS DE GRADO

Previa a la obtención del Título de:

DIPLOMA SUPERIOR EN AUDITORIA INFORMATICA

Presentado por

Ing. Catania Játiva Vásconez

Lsi. Ma. Verónica Chávez

Guayaquil - Ecuador

2011

AGRADECIMIENTO

ING. SOCRATES DUEÑAS

Director de tesis, por su ayuda y colaboración para la realización de este trabajo.

Entidad Educativa por el apoyo durante la ejecución del proceso.

DEDICATORIA

A Dios por su infinita bondad, quien nos dio la fe, fortaleza y salud para realizar este trabajo.

A nuestras familias por su apoyo para alcanzar esta meta y ser la base de nuestras vidas.

TRIBUNAL GRADUACIÓN

Ing. Jorge Olaya
DIRECTOR DEL DIPLOMADO

Ing. Sócrates Dueñas
DIRECTOR DE TESIS

Ing. Antonio Márquez
MIEMBRO DEL TRIBUNAL

DECLARACION EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

{Reglamento de Graduación de la ESPOL}

Catania Játiva

Ing. Catania Játiva Vásquez

Lsi. Verónica Chávez

Lsi. Ma. Verónica Chávez.

RESUMEN

El presente proyecto establece la elaboración de una auditoria del proceso de Facturación que se ha identificado entre los más críticos de la instrucción educativa en la hemos elaborado nuestra tesis de graduación.

Se ha realizado una revisión sobre los controles internos establecidos en la institución para este proceso, utilizando metodologías y normas que nos han proporcionado los lineamientos para lograr identificar la efectividad o deficiencia de los mismos.

Como resultado se presenta un informe que contiene la opinión sobre la seguridad razonable acerca del diseño y operación de controles definidos en el proceso. Así también se han elaborado recomendaciones sobre el control interno que servirán como oportunidades de mejora para la institución.

INDICE GENERAL

AGRADECIMIENTO	1
DEDICATORIA.....	2
TRIBUNAL GRADUACIÓN	3
DECLARACION EXPRESA	4
RESUMEN.....	5
CAPITULO I.....	10
INTRODUCCIÓN.....	10
ANTECEDENTES.....	10
INTRODUCCIÓN AL CONTROL INTERNO	12
INTRODUCCIÓN A LA AUDITORIA DE PROCESOS	14
OBJETIVOS	17
METODOLOGÍAS, ESTÁNDARES Y PROCEDIMIENTOS	19
METODOLOGÍA DE TRABAJO	25
PRINCIPALES IMPEDIMENTOS	25
EQUIPO DE TRABAJO.....	26
PLAN GENERAL DEL PROYECTO	27
OBSERVACIONES ADICIONALES	27
CAPITULO II.....	28
ENTENDIMIENTO DEL AMBIENTE DE CONTROL INTERNO DE LA ENTIDAD EDUCATIVA.....	28
INFORMACION GENERAL DE LA ENTIDAD EDUCATIVA	28
ORGANIGRAMA INSTITUCIONAL.....	29
ORGANIGRAMA SEDE.....	30
FACTORES EVALUADOS DEL CONTROL INTERNO	32
COMUNICACIÓN Y EJECUCIÓN DE INTEGRIDAD Y VALORES ÉTICOS	32

PROCESO DE GOVERNABILIDAD.....	34
FILOSOFÍA DE LA ADMINISTRACIÓN Y ESTILO DE OPERACIÓN.....	35
ESTRUCTURA ORGANIZACIONAL Y COMPROMISO PARA LA COMPETENCIA.....	37
ASIGNACIÓN DE AUTORIDAD Y RESPONSABILIDAD.....	38
POLÍTICAS Y PRÁCTICAS DE RECURSOS HUMANOS.....	38
PROCESO DE FACTURACION DE LA ENTIDAD EDUCATIVA.....	39
SUB-PROCESOS.....	39
SUB-PROCESO: PRE – FACTURACIÓN.....	39
SUB-PROCESO: GENERACIÓN DE ARCHIVO PARA RECAUDACIÓN.....	42
SUB-PROCESO: CARGA DE ARCHIVO DE RECAUDACIONES.....	44
SUB-PROCESO: GENERACIÓN DE CONVENIOS.....	46
SUB-PROCESO: DEPURACION DE CUPOS.....	48
SUB-PROCESO: MATRÍCULAS EXTRAORDINARIAS.....	49
DETALLE DE HERRAMIENTAS.....	50
FLUJOS DEL PROCESO.....	52
ENTENDIMIENTO DEL AREA DE TECNOLOGIA.....	54
INFORMACION GENERAL DE LA ENTIDAD EUCATIVA.....	54
GESTIÓN DE TI.....	55
ORGANIZACIÓN DE TI.....	56
POLITICAS Y PROCEDIMIENTOS DE TI.....	62
MANEJO DEL RIESGO DE TI.....	64
INFRAESTRUCTURA DE TI.....	66
ENTENDIMIENTO DE CONTROLES DE TI.....	70
GESTIÓN DE LA SEGURIDAD DE TI.....	70
GESTIÓN DE LAS OPERACIONES DE TI.....	75
GESTIÓN DE CAMBIOS A PROGRAMAS.....	80
GESTIÓN DE DERROLLO DE SISTEMAS.....	81

EVALUACIÓN DE ESTRUCTURA DE RIESGOS/ CONTROLES.....	83
SIGNIFICADO DE LA EVALUACIÓN DE RIESGOS.....	83
ESTRUCTURA DE LA EVALUACIÓN DE RIESGOS	83
CLASIFICACIÓN DE LOS RIESGOS.....	85
EVALUACION DE RIESGOS CONTROL INTERNO.....	86
En base a nuestra comprensión y evaluación de Riesgos del Marco de Control Interno determinamos un enfoque de no confort en controles de TI, no obstante el control interno en cuanto al ambiente sobre el cual opera la institución no presenta aspectos relevantes que observar.	87
EVALUACION DE RIESGOS EN TI.....	88
CONCLUSIONES DE LA EVALUACION DE RIESGOS.	89
IDENTIFICACIÓN DE CONTROL.....	90
PROGRAMA DE AUDITORÍA INFORMÁTICA DE LA ENTIDAD EDUCATIVA	93
OBJETIVO	93
ALCANCE	93
METODOLOGÍA	94
RESPONSABLES.....	95
PROCEDIMIENTOS DE AUDITORIA	96
PLAN DE AUDITORIA.....	97
EVALUACIÓN DE CONTROLES	100
NATURALEZA DE LAS PRUEBAS DE CONTROLES	100
ALCANCE DE LAS PRUEBAS DE CONTROLES.....	100
NATURALEZA DE LOS CONTROLES MANUALES Y AUTOMATIZADOS	101
INFORME	111
CONCLUSIONES Y RECOMENDACIONES	112
CONCLUSIONES:	112
RECOMENDACIONES:	113
ANEXOS.....	114

ANEXO I: EVALUACIÓN DE AMBIENTE DE CONTROL DEL PROCESO DE FACTURACIÓN.....	115
ANEXO II: MATRIZ DE RIESGO DE TI	120

CAPITULO I

INTRODUCCIÓN

ANTECEDENTES

“El gran reto acerca de crear el futuro no es predecirlo. La meta es tratar de imaginar un futuro que sea verosímil: el futuro que podemos crear. Para ese efecto, las nuevas herramientas de estrategia tienen que echar raíces porque no se puede crear el futuro utilizando las viejas herramientas de estrategia.

El esfuerzo que realiza para crear un punto de vista sobre el futuro y una estrategia para manejar el cambio, representa la capacidad de desarrollar un sentido profundo de discontinuidades para crear una jerarquía de imaginación”.

Gary Hamel

Una buena administración de negocios incluye todos los procesos principales y de soporte que tienen las empresas para alcanzar las metas organizacionales; los mismos deben de ser definidos y evaluados periódicamente por la organización y revisores externos, para asegurar su correcto funcionamiento.

La base de la gestión de las empresas actualmente se soporta altamente en la tecnología, la cual, debe estar normada y controlada para poder brindar un marco de asegure la disponibilidad, integridad y exactitud de los procesos que se llevan a cabo bajo un ambiente informático.

En este sentido, se hace necesario poner énfasis en la auditoría a los procesos principales de las empresas e instituciones que son vistos como la esencia del negocio, no solamente porque la mayoría del trabajo se logra mediante ellos, sino porque los procesos son los factores que realmente hacen diferentes a las empresas.

Por lo tanto, el presente proyecto de graduación del diplomado de Auditoría Informática tiene como objetivo contribuir activamente con un trabajo de auditoría que determine el correcto funcionamiento del proceso de Facturación que se soporta en un entorno tecnológico, de una prestigiosa entidad educativa de nuestro país.

INTRODUCCIÓN AL CONTROL INTERNO

DEFINICIÓN DE CONTROL INTERNO

La SEC define el control interno (utilizando un marco de referencia conocido como COSO(1)) como un proceso efectuado por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Fiabilidad de la información financiera.
- Cumplimiento de las leyes y normas aplicables.

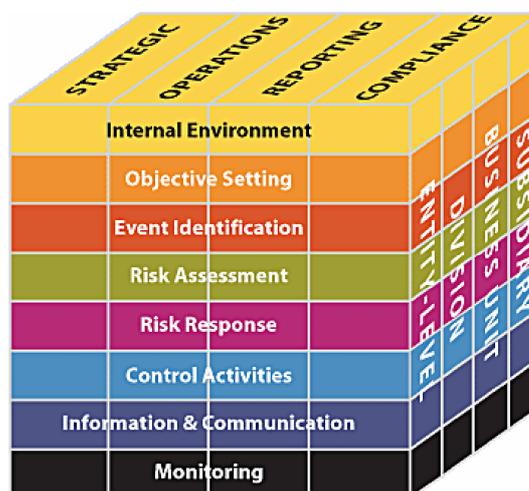
La sección 404 de la SOX se refiere a los controles necesarios para asegurar la fiabilidad de la información financiera y el cumplimiento de las leyes y regulaciones aplicables.

DEFINICIÓN DE DEFICIENCIAS

Una deficiencia de control existe cuando el diseño u operación de un control no permite a la gerencia o a los empleados, en el curso normal de sus funciones asignadas, prevenir o detectar errores oportunamente.

COMPONENTES DE CONTROL

Un marco de control interno de la entidad consta de cinco componentes interrelacionados que pueden ser aplicados en cualquier nivel de la organización.



INTRODUCCIÓN A LA AUDITORIA DE PROCESOS

DEFINICIÓN DE PROCESO

Es un conjunto de actividades secuenciales que se interrelacionan entre sí para llevar a cabo una actividad o lograr un objetivo.



IMPORTANCIA DEL ENFOQUE DE LOS PROCESOS

Todas las actividades de la empresa constituyen procesos o subprocesos, cada uno representa costos que deben ser correctamente invertidos. Es decir, si un proceso no tiene controles correctamente diseñados o no cuenta con ellos, podría incurrir en mayores costos para la empresa por pérdidas financieras, pérdida de imagen por errores o fraudes en los procesos de negocio y más aun inconformidad de clientes al mantener procesos deficientes.

AUDITORIA DE PROCESOS

Se ha desarrollado una serie de conceptos que intentan describir el ambiente externo e interno en que operan las organizaciones, para entender el contexto básico en que se desarrolla la Gestión Gerencial y comprender que los factores claves para alcanzar, mantener y elevar la competitividad de las empresa reside en última instancia en implementar los cambios y las mejoras necesarias a los procesos.

Teniendo en cuenta lo anterior adquiere especial importancia la auditoría a los procesos de la empresa para responder correctamente a las expectativas y necesidades de la Alta Gerencia.

El planeamiento de la auditoría a los procesos debe identificar los procesos que resultan críticos para el logro de los objetivos estratégicos empresariales.

En la selección de los procesos a ser auditados debe tomarse en cuenta las siguientes razones:

- a. Alto impacto en los ingresos de la empresa.
- b. Relacionados con la imagen empresarial y su reputación institucional.
- c. Que afecten directamente la relación con el cliente.
- d. Procesos de alto costo e ineficiencias en el uso de recursos.

- e. Procesos con tiempo de ciclos prolongados.
- f. Problemas y/o quejas de los clientes externos e internos.
- g. Impactados por la Existencia de nuevas tecnologías.

OBJETIVOS

El objetivo de la tesis es la ejecución de un proceso de auditoría al ciclo de facturación en las secciones que involucra a la tecnología para una institución educativa, basado en un análisis del ciclo y su entorno tecnológico, poniendo en práctica los conocimientos adquiridos durante el Diplomado de Auditoría Informática.

Como objetivo adicional pero no menos relevante, contribuir con la institución presentando un informe de auditoría que contenga nuestra opinión sobre el diseño y efectividad de los controles, así como, recomendaciones que permitan mejorar el control y seguridad del proceso de facturación y el entorno tecnológico que lo soporta.

ALCANCE

El Alcance del proyecto comprende en examinar el ambiente de control en el que se desarrolla el ciclo de facturación para los cobros realizados a los estudiantes de la entidad educativa para lo que se van a incluir actividades de análisis y pruebas de cumplimiento de los controles establecidos en este proceso.

Se entregara un informe final en el que se incluirán las observaciones identificadas de nuestra auditoria, así como recomendaciones bajo un enfoque de mejores prácticas para contribuir con las mejoras a nivel del proceso como de tecnología.

Cabe indicar que en el presente trabajo no se incluirá diseño ni implementación de los controles sugeridos.

METODOLOGÍAS, ESTÁNDARES Y PROCEDIMIENTOS

Para nuestro proceso utilizaremos como marco referencial las Normas Ecuatorianas de Auditoría (NEA) que nos proporcionaran las pautas para elaborar la revisión.

Adicionalmente utilizaremos otros estándares y metodologías para apoyar nuestro proceso de revisión y emisión de recomendaciones, tales como: ISACA, ISO 9001:2008, COBIT 4.1, ITIL v3.

NORMAS ECUATORIANAS DE AUDITORIA (NEA)

El propósito de esta Norma Ecuatoriana sobre Auditoría (NEA) es establecer normas y dar lineamientos sobre el objetivo y los principios generales que amparan una auditoría de estados financieros.

LEY SARBANES-OXLEY

En los Estados Unidos de América surge la ley Sarbanes-Oxley, la cual debe su nombre a los dos congresistas que contribuyeron a su redacción. La ley establece la creación de un Comité de Vigilancia de la Contabilidad de las Empresas Públicas (en adelante el Comité), cuyas funciones entre otras, son "...proteger el

interés de los inversores, y más allá, el interés público, en la preparación de reportes de auditoría informativos, exactos e independientes”.

El cumplimiento de las regulaciones establecidas en la ley por parte de las distintas empresas, se convierte en una especie de “sello de confianza” requerido por los inversores.

COSO – MARCO DE CONTROL INTERNO REFERENCIAL

Proporciona un marco adecuado y disponible para propósitos de la evaluación de la gerencia. El marco de referencia identifica tres objetivos principales del control interno: eficiencia y efectividad de las operaciones, información financiera y cumplimiento de las leyes y regulaciones.

ISACA

Organización global que establece las pautas para los profesionales del gobierno, control, seguridad y auditoría de información. Sus normas de auditoría y control de la Seguridad de Información son seguidos por profesionales de todo el mundo y sus investigaciones abordan temas profesionales que son desafíos para sus constituyentes.

SISTEMAS DE GESTIÓN DE LA CALIDAD ISO 9001:2008

La Norma ISO 9001 especifica los requisitos para un buen sistema de gestión de la calidad que pueden utilizarse para su aplicación interna por las organizaciones, para certificación o con fines contractuales. La norma ISO 9001 tiene origen en la norma BS 5750.

La ISO 9001:2008 es válida para cualquier organización, independientemente de su tamaño o sector, que busque mejorar la manera en que se trabaja y funciona. Además, los mejores retornos en la inversión, vienen de compañías preparadas para implantar la citada normativa en cualquier parte de su organización.

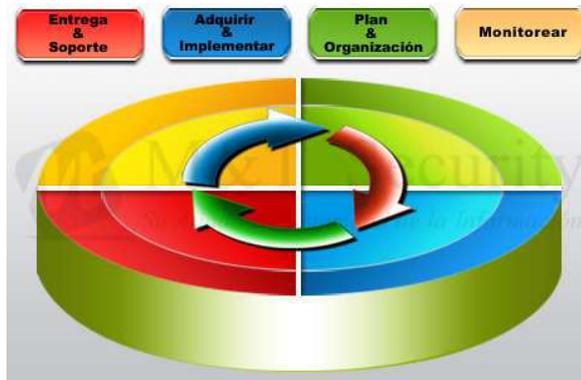


COBIT V 4.1

COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los Interesados (Stakeholders).

COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares.

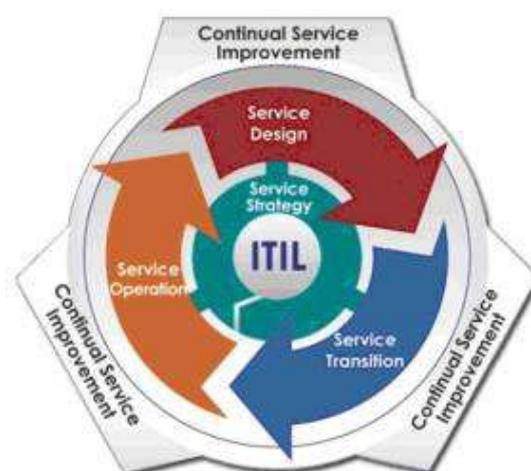
Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de la misma.



ITIL V3

Un conjunto de guías de mejores prácticas para la Gestión de Servicios TI. ITIL es propiedad de la OGC y se compone de una serie de publicaciones que ofrece asesoramiento sobre la provisión de calidad de TI Servicios, y en los procesos y las instalaciones necesarias para apoyo a ellos.

El núcleo de la estructura de esta práctica se materializa en un Ciclo de Vida de servicio que es iterativo y multidimensional. Que proporciona una estructura, estabilidad y fuerza al servicio de gestión de capacidades con sólidos principios, métodos y herramientas. Esto sirve para proteger las inversiones y proporcionar la base necesaria para la medición, el aprendizaje y la mejora continua.



METODOLOGÍA DE TRABAJO

La metodología de trabajo que manejaremos es inductiva, que nos permite por medio de la observación experimental en sitio analizar los hechos que se presenten durante el proyecto y poder generar conclusiones que aporten significativamente a la mejora del control interno de la institución educativa en los puntos que evaluaremos.

PRINCIPALES IMPEDIMENTOS

Los principales impedimentos de nuestro proyecto se relacionan con la seguridad de la información de la institución educativa que nos brinda la oportunidad de realizar nuestro proyecto, debido a que por temas de salvaguardar la información que para la entidad es categorizada como confidencial no se nos permitirá realizar capturas de pantallas de los resultados de las pruebas y no se podrá realizar re-procesos de información de acuerdo a lo definido inicialmente con el responsable de Sistemas.

EQUIPO DE TRABAJO

Se ha asignado un recurso para el trabajo de auditoría y cuyas responsabilidades son:

NOMBRES	TITULO ACADÉMICO	CARGO
María Verónica Chávez	Licenciada en Sistemas de Información	Auditora de Sistemas – Líder del Equipo
Catania Játiva Vásquez	Ingeniera en Sistemas	Auditora de Sistemas

PLAN GENERAL DEL PROYECTO

- 1.1. Objetivo y Alcance del Proyecto
- 1.2. Identificar las Restricciones del Proyecto
- 1.3. Entendimiento del ambiente de control
- 1.4. Análisis de riesgos del ambiente de control
- 1.5. Determinación de los controles a nivel del proceso de Facturación
- 1.6. Evaluación de la eficacia operativa de las actividades de control
- 1.7. Informe

OBSERVACIONES ADICIONALES

Ninguna

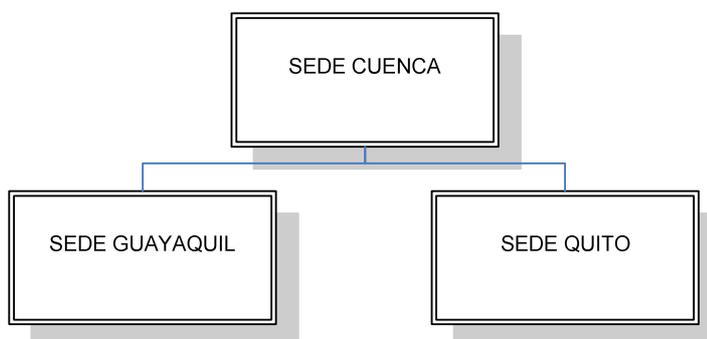
CAPITULO II

ENTENDIMIENTO DEL AMBIENTE DE CONTROL INTERNO DE LA ENTIDAD EDUCATIVA

El documento en el cual se detalla el proceso de facturación va a contener información relevante sobre el ambiente de control sobre el que se ejecuta el mismo, los sub-procesos y actividades de control, con la finalidad de identificar los controles claves existentes a nivel de cumplimiento y eficacia de los mismos.

INFORMACION GENERAL DE LA ENTIDAD EDUCATIVA

La entidad educativa actualmente brinda el servicio de educación tanto en carreras de pre-grado como de post-grado a nivel nacional en sus tres sedes.



La sede principal se encuentra en Cuenca donde se encuentra la mayor oferta educativa, en la ciudad de Guayaquil se encuentra un campus y en la ciudad de Quito se encuentran 2 campus.

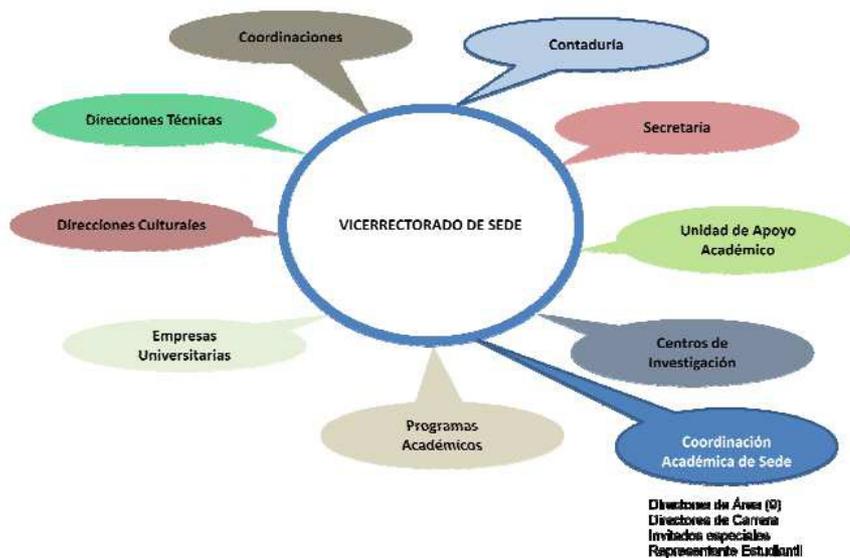
La información relacionada al proceso de facturación que es generada por las aplicaciones se maneja de manera centralizada en la sede de Cuenca.

Los procesos operativos son descentralizados ya que en cada una de las sedes se maneja niveles de autorización independiente, siendo la máxima autoridad en cada de las sedes el Vice-rector de las mismas

ORGANIGRAMA INSTITUCIONAL



ORGANIGRAMA SEDE



FACTORES EVALUADOS DEL CONTROL INTERNO

COMUNICACIÓN Y EJECUCIÓN DE INTEGRIDAD Y VALORES ÉTICOS

CÓDIGOS DE CONDUCTA, COMPORTAMIENTO ÉTICO Y MORAL.

La entidad educativa dentro de su documentación formal cuenta con políticas claras sobre códigos de conducta y sanciones a las cuales se someten en caso de incumplimiento del mismo.

El documento que registra dichas políticas se encuentra debidamente registrado, aprobado por las autoridades correspondientes, y publicado en medios de fácil acceso para el personal administrativo y de servicios como es la página de la entidad educativa.

PRÁCTICAS DE NEGOCIO ACEPTABLES.

El desarrollo de las actividades de la entidad educativa se encuentra regulado y normado en base a políticas internas que se detallan en los estatutos y reglamentos de la misma.

Adicionalmente cuenta con organismos de control externo (CONAE) que norman las actividades y procesos de acreditación.

***RELACIONES CON EMPLEADOS, PROVEEDORES,
COMPETIDORES, ENTES DE CONTROL, INVERSIONISTAS.***

La entidad educativa tiene claramente identificada las acciones permitidas y aquellas que no son autorizadas en sus relaciones con sus proveedores, competidores, y entes de control. Las políticas se encuentran definidas en documentos que están publicados y difundidos por medios como la página web de la institución educativa.

INCENTIVOS Y TENTACIONES

Las actividades que se identifican como críticas en el proceso de facturación no tienen una adecuada segregación de funciones, considerando que la generación de los archivos mediante la cual se realiza el cobro de valores por concepto de colegiatura y matrícula lo realiza la misma persona que cobra, adicionalmente este archivo no reposa en un lugar que mantenga las seguridades en cuanto a modificaciones de la información.

La carga del archivo mediante el cual se informa a los bancos los valores que deben ser recaudados es depositada en cada una de las dos entidades financieras que realizan la recaudación sin requerir una aprobación ni validación operativa.

Las políticas establecidas en el Reglamento del personal Administrativo y Servicios tiene claramente publicado y establecido los incentivos monetarios y de crecimientos profesional para el personal que labora en la entidad educativa.

PROCESO DE GOBERNABILIDAD

INDEPENDENCIA FRENTE A LA ADMINISTRACIÓN.

La entidad educativa cuenta con un plan estratégico actualizado al año 2011 que se encuentra aprobado y publicado, donde se detallan fechas y actividades a ejecutarse para el cumplimiento de las metas institucionales.

FRECUENCIA Y OPORTUNIDAD DE LAS REUNIONES DEL CONSEJO SUPERIOR.

En la documentación analizada se refleja las condiciones y pasos a seguir para solicitar reuniones a nivel del consejo superior, adicionalmente existe una agenda con fechas fijas en las cuales se tiene programadas reuniones del consejo superior.

***SUFICIENCIA Y OPORTUNIDAD DE LA INFORMACIÓN QUE SE
SOMETE A EVALUACIÓN***

La entidad educativa cuenta con área de auditoría financiera interna; la misma que dentro de la planificación anual tiene definida fechas periódicas para la revisión de información generada en los procesos de la entidad educativa.

FILOSOFÍA DE LA ADMINISTRACIÓN Y ESTILO DE OPERACIÓN.

NATURALEZA DE LOS RIESGOS DE NEGOCIOS ACEPTADOS

La entidad educativa no cuenta con políticas en lo referente al manejo de riesgos, en la medida que estos se presentan o materializan son analizados y mitigados en función de la experiencia de la persona, mas no en función de políticas previamente establecidas.

ACTITUDES Y ACCIONES FRENTE A LA INFORMACIÓN FINANCIERA.

La información que detalla resultados financieros es manejada con mucho sigilo y no es de fácil acceso para todas las personas, y en caso de ser requerida debe cumplir con proceso de autorizaciones de los niveles pertinentes.

Es importante indicar que información que registra los pagos de los estudiantes es modificada para poder ser cargada en el sistema de la entidad educativa. La modificación de la información se realiza porque el sistema controla que no se pueda realizar la carga de un pago con el mismo código de cobro más de una vez; este escenario se presenta cuando un estudiante realiza pagos parciales en las ventanillas de las instituciones financieras.

ESTRUCTURA ORGANIZACIONAL Y COMPROMISO PARA LA COMPETENCIA

DEFINICIÓN DE ÁREAS CLAVES DE AUTORIDAD Y

ESTABLECIMIENTO DE LÍNEAS APROPIADAS DE INFORMACIÓN

La entidad educativa cuenta con una estructura que le permite soportar la operatividad administrativa de la misma, adicionalmente se encuentran claramente definidas y divulgadas las funciones de cada una de estas.

Las funciones del personal que forma parte de la alta administración son claras y son parte de la documentación que es revisada y calificada por los organismos de control.

CLARIDAD EN EL CONOCIMIENTO Y EXPERIENCIA DE LOS ADMINISTRADORES A LA LUZ DE SUS RESPONSABILIDADES.

Existe claramente definido el perfil y la capacitación necesaria que debe tener la persona que aplique a cualquiera de las funciones del personal administrativo.

La entidad educativa cuenta con planes de capacitación y beneficios a nivel económico para su personal que aplique a estudios que les permita perfeccionarse y mantenerse actualizados en los temas relacionados a sus funciones.

ASIGNACIÓN DE AUTORIDAD Y RESPONSABILIDAD

La asignación de las responsabilidades de la alta administración se encuentra claramente definida y en ellas se incluye la responsabilidad de mantener y gestionar el control interno de la entidad educativa.

POLÍTICAS Y PRÁCTICAS DE RECURSOS HUMANOS

Las políticas bajo las cuales se administra el recurso humano se encuentran claramente especificadas en los reglamentos de cada uno de los tipos de personal, estos se encuentran publicados en el sitio web de la entidad educativa.

La cultura organizacional bajo la cual se administra y dirige la entidad educativa es claramente detallada en los documentos formales de la misma; así como difundida por varios medios a todo nivel de la organización.

Es importante que el proceso de reclutamiento para nuevas posiciones o vacantes se realice de forma interna considerando el capital humano uno de sus mayores contingentes.

PROCESO DE FACTURACION DE LA ENTIDAD EDUCATIVA

SUB-PROCESOS

SUB-PROCESO: PRE – FACTURACIÓN

ENTRADAS DEL SUB-PROCESO.

Las entradas que inician el proceso de facturación son:

- Registro de estudiantes en secretaria
- Registro de estudiantes mediante la página web www.ups.eu.ec

ACTIVIDADES DEL SUB-PROCESO

El proceso de facturación toma datos de los estudiantes y de los registros realizados mediante sus dos canales definidos anteriormente.

El proceso realiza el cálculo de forma automática el costo total del registro, calculando en base a la cantidad de créditos de cada materia. El costo por crédito está relacionado al quintil en el cual fue ubicado el estudiante acorde a su nivel socio económico.

Los rubros que son considerados para la facturación son:

- Matrícula
- Curso de Inglés
- Valor de los créditos tomados por los estudiantes

El valor total a recaudar considera adicionalmente descuentos; el descuento actual que se aplica a todos los estudiantes es un subsidio del gobierno, el mismo que se detalla también en la factura.

El monto total por cada estudiante es recaudado en pagos parciales; el número de pagos parciales varían por cada una de las sedes como se refleja en la siguiente tabla:

SEDE	NUMERO DE PAGOS
Cuenca	3
Quito	3
Guayaquil	5

La recaudación de los siguientes pagos se la realiza mediante el mismo proceso con la diferencia que esta información no tiene fecha de caducidad permitiendo que la recaudación se realice en cualquier momento.

COMPONENTES DE SUB-PROCESO

PARTICIPANTES	HERRAMIENTAS
Estudiantes	SNA
Tesorera-Cajera	SIGAC

SALIDAS DEL SUB-PROCESO

Registro de estudiantes

Pre-Facturas

SUB-PROCESO: GENERACIÓN DE ARCHIVO PARA RECAUDACIÓN

ENTRADAS DEL SUB-PROCESO.

Registro de Estudiantes

ACTIVIDADES DEL SUB-PROCESO

El sistema toma la información de los estudiantes registrados y genera archivos donde se detallan datos que permite la recaudación de estos valores en los dos canales de cobros, estos archivos son de tipo texto separados por tabuladores.

Estos archivos son cargados en el portal transaccional de los bancos donde la entidad educativa tiene convenio y son:

- Pichincha
- Produbanco.

La información generada en el período de matriculas ordinarias tienen periodo de caducidad; una vez culminado el período de vigencia los estudiantes el pago no es permitido en los bancos, y el estudiante debe realizar un nuevo proceso de matriculación con carácter de extraordinario.

COMPONENTES DE SUB-PROCESO

PARTICIPANTES	HERRAMIENTAS
Estudiantes	SIGAC
Tesorera-Cajera	Pagina web del banco
Entidades financieras	

SALIDAS DEL SUB-PROCESO

Archivos para recaudaciones

SUB-PROCESO: CARGA DE ARCHIVO DE RECAUDACIONES.

ENTRADAS DEL SUB-PROCESO.

Archivo de recaudaciones.

ACTIVIDADES DEL SUB-PROCESO

La tesorera de cada una de las sedes procede diariamente a cargar los archivos de las recaudaciones realizadas por cada una de las instituciones financieras en el sistema SIGAC para proceder con la actualización de los pagos realizados.

Una vez realiza la carga se procede con la impresión de las facturas que serán entregadas cuando el estudiante se acerque a las ventanillas de la entidad educativa.

COMPONENTES DEL SUB-PROCESO

PARTICIPANTES	HERRAMIENTAS
Tesorera-Cajera	SIGAC
Entidades financieras	Página web del banco

SALIDAS DEL SUB-PROCESO

Facturas

SUB-PROCESO: GENERACIÓN DE CONVENIOS

ENTRADAS DEL SUB-PROCESO.

Solicitudes de aprobación de convenio.

ACTIVIDADES DEL SUB-PROCESO.

El proceso de recaudaciones contempla solamente pagos totales por tal motivo los estudiantes que realizan pagos parciales deben entregar una solicitud para aprobación de convenios mediante los cuales se les autoriza que el valor del pago sea realizado de manera fraccionaria.

El departamento de bienestar estudiantil, registra los convenios aprobados en una hoja Excel, el mismo en que se detalla las fechas de pago de los siguientes abonos de la cuota inicial.

El archivo es custodiado por el departamento de contabilidad y son los que realizan la gestión de cobro.

COMPONENTES DEL SUB-PROCESO

PARTICIPANTES	HERRAMIENTAS
Tesorera-Cajera	SIGAC
Estudiante	Excel
Vice-rector	

SALIDAS DEL SUB-PROCESO

Convenios Aprobados

Comprobantes de Pago

Facturas.

SUB-PROCESO: DEPURACION DE CUPOS***ENTRADAS DEL SUB-PROCESO.***

Pagos actualizados.

ACTIVIDADES DEL SUB-PROCESO.

Una vez culminado el proceso de matriculación en período ordinario se ejecuta el proceso de liberación de cupos donde se depuran las pre-facturaciones que no han recibido un pago o no tienen registrado un convenio.

COMPONENTES DEL SUB-PROCESO

PARTICIPANTES	HERRAMIENTAS
Tesorera-Cajera	SIGAC

SALIDAS DEL SUB-PROCESO

Disponibilidad de cupos.

SUB-PROCESO: MATRÍCULAS EXTRAORDINARIAS

ENTRADAS DEL SUB-PROCESO.

- Registro de estudiantes en secretaria

ACTIVIDADES DEL SUB-PROCESO.

El proceso extraordinario de matriculas se habilita una vez el ordinario terminó y se realiza el sub-proceso de recaudaciones de recaudación.

La información generada para esta recaudación no tiene fecha de caducidad.

COMPONENTES DEL SUB-PROCESO

PARTICIPANTES	HERRAMIENTAS
Tesorera-Cajera	SIGAC
Estudiante	SNA

SALIDAS DEL SUB-PROCESO

Archivos.

DETALLE DE HERRAMIENTAS

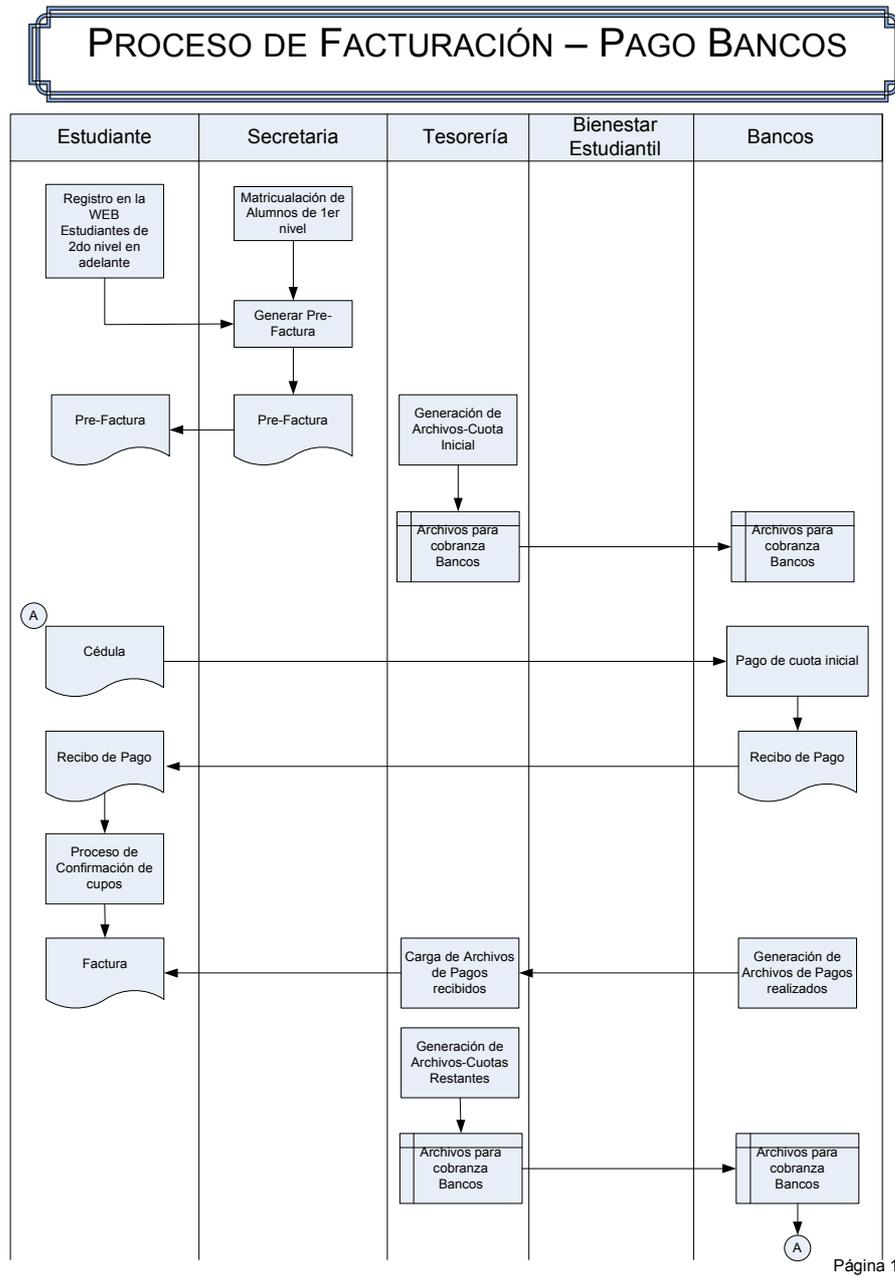
SNA: Sistema Nacional Administrativo, que permite el registro de los estudiantes de 1er nivel.

SIGAC: Sistema Integrado de gestión administrativa y contable, este aplicativo permite realizar varias actividades financieras mediante los módulos como:

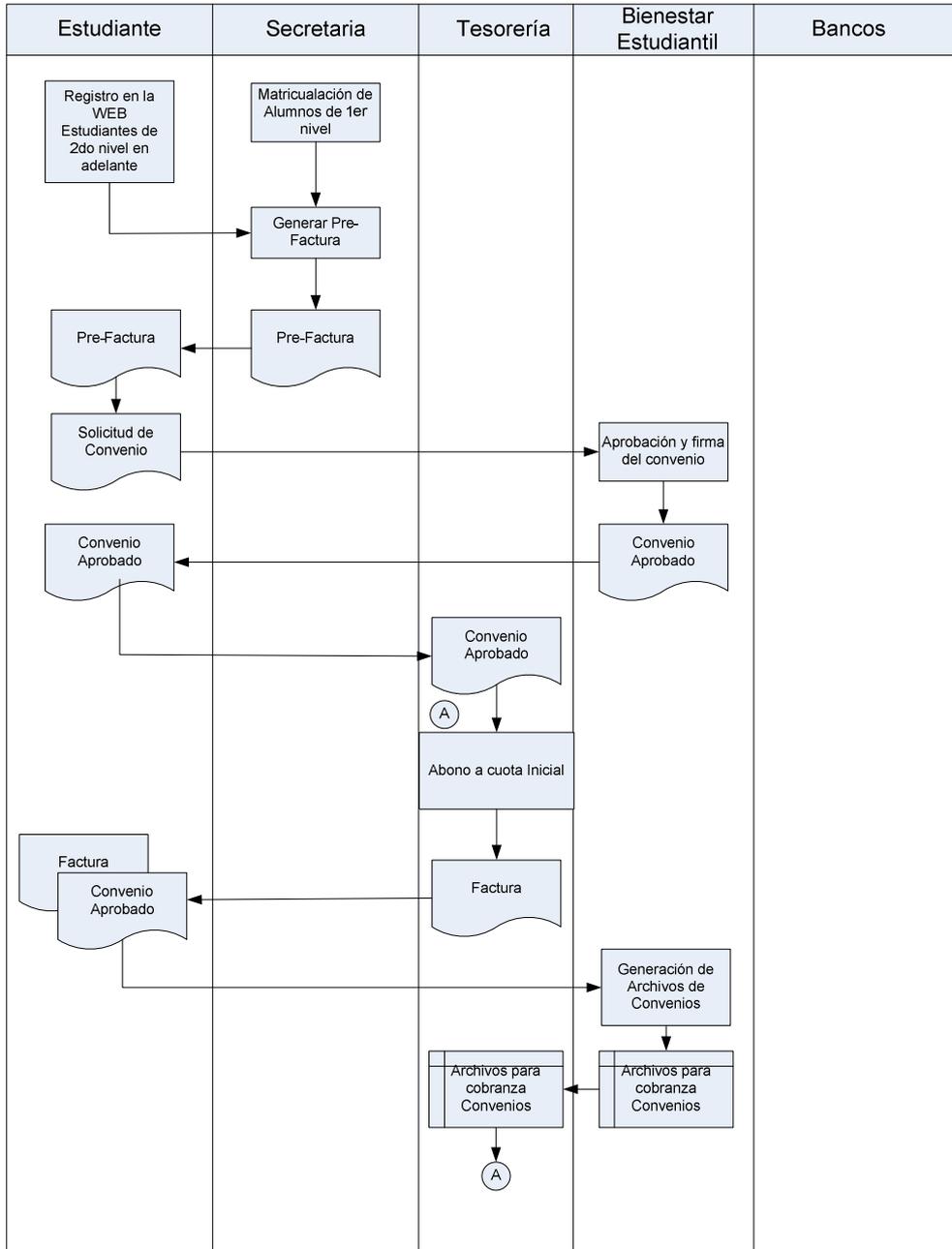
- Activo Fijo
- Administrativo
- Conciliación
- Contable.
- Control de pagos.
- Facturación.
- Flujo de caja.
- Inventario.
- Tesorería.
- Ventas.
- Clientes.

www.ups.eu.ec: Permite el registro de los estudiantes del 2do nivel hasta el 8vo, adicionalmente tiene funcionalidades como detalle de deudas pendientes, consulta de tareas y consulta de calificaciones.

FLUJOS DEL PROCESO



PROCESO DE FACTURACIÓN – CONVENIOS

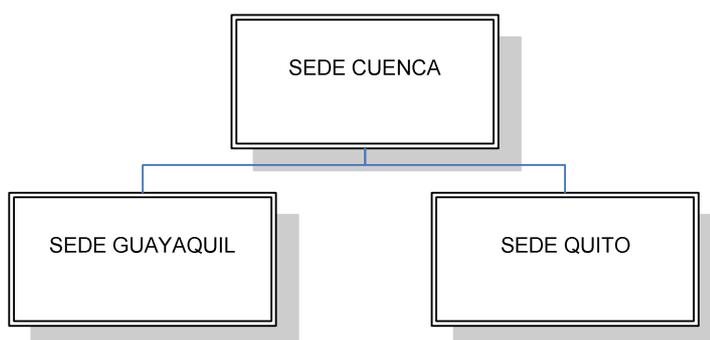


ENTENDIMIENTO DEL AREA DE TECNOLOGIA

El documento de entendimiento de TI va a contener información relevante sobre el manejo del ambiente de tecnología de información, con la finalidad de identificar los controles claves existentes a nivel de la gestión del entorno de TI y los Controles Generales TI, a fin de determinar la seguridad en controles que tiene la institución en su ambiente de control a nivel de TI.

INFORMACION GENERAL DE LA ENTIDAD EUCATIVA

La entidad educativa actualmente brinda el servicio de educación tanto en carreras de pre-grado como de post-grado a nivel nacional en sus tres sedes.



La sede principal se encuentra en Cuenca donde se encuentra la mayor oferta educativa, en la ciudad de Guayaquil se encuentra un campus y en la ciudad de Quito se encuentran 2 campus.

En la sede principal, se encuentran concentradas las operaciones de TI.

GESTIÓN DE TI

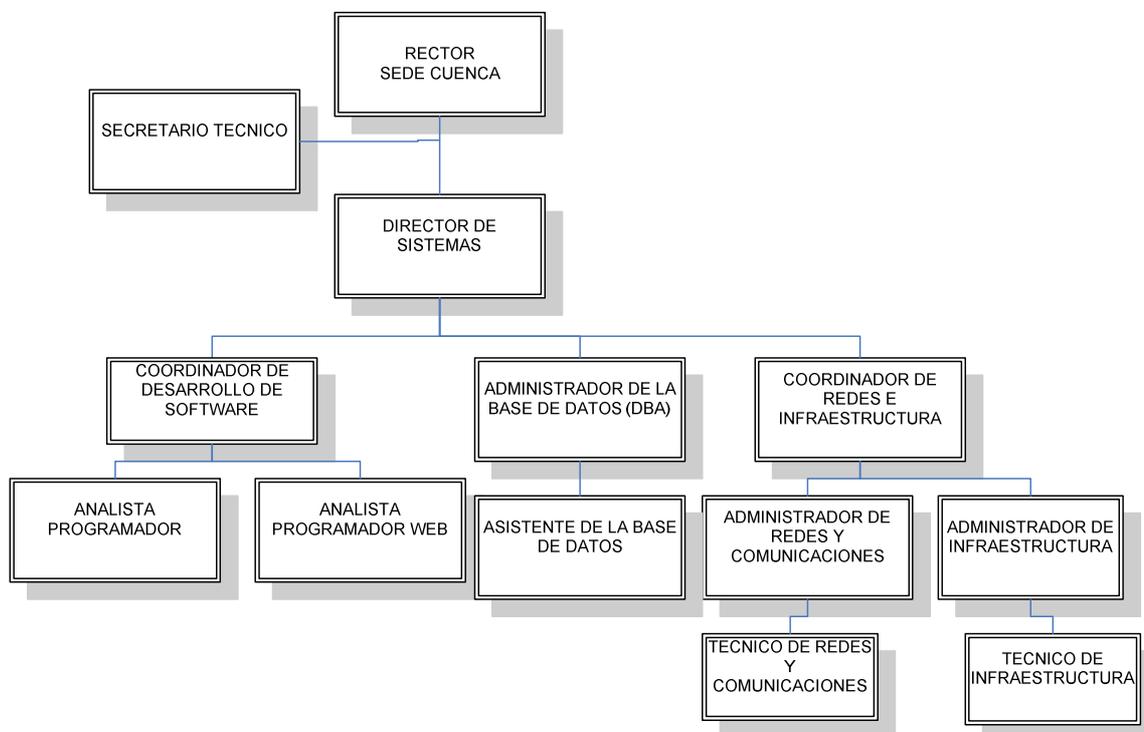
PLANIFICACIÓN DE TI

Se identifica que para el año 2010 existía un presupuesto para el área de TI, actualmente para el año 2011 no existe conocimiento de presupuesto asignado, siendo la forma de operar en caso de requerimientos de inversiones tecnológicas realizar solicitudes al vicerector general quien emite la aprobación de la misma.

En lo relacionado a la gestión de nuevos proyectos se realiza bajo demanda operativa, la misma que es presentada ante del Secretario técnico quien evaluará el proyecto y realizar la recomendación respectiva ante el vice-rector general

ORGANIZACIÓN DE TI

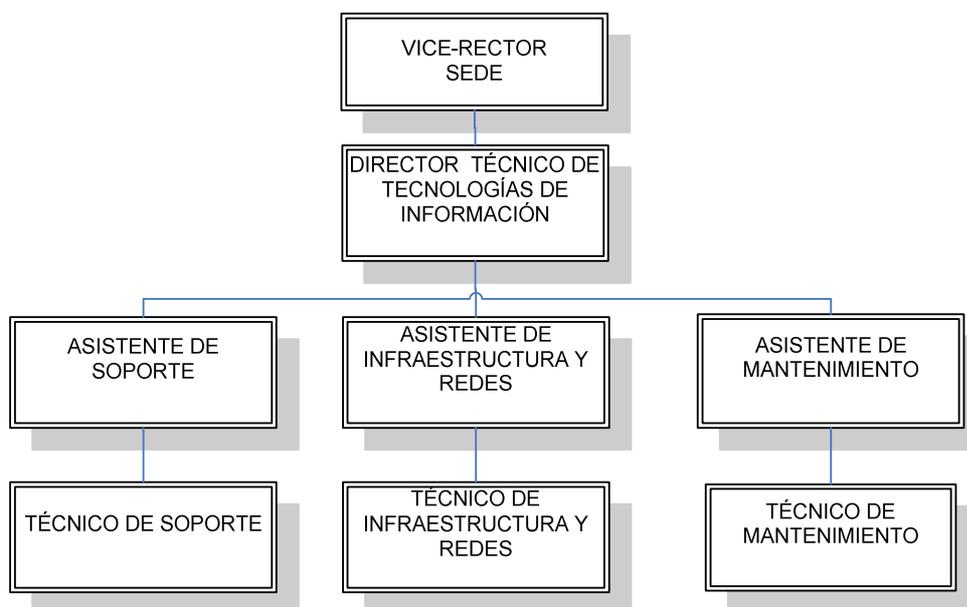
La parte administrativa del área de TI en la sede principal de Cuenca se encuentra constituida por 14 personas a cargo del Director de sistemas y se encuentra estructurada de la siguiente manera:



En cada una de las otras sedes se encuentran estructuras de TI, que soportan en las siguientes actividades:

- ✓ Soporte a usuarios
- ✓ Administración de las seguridades.
- ✓ Administración de la Infraestructura.

Cada sede reporta al Vicerrectorado de cada una de ellas. Este año se realizó un cambio en la estructura organizacional, en la división de funciones entre el Secretario Técnico y el Director de Sistemas, ya que antes las funciones de estos dos cargos eran centralizados en una sola persona.



FUNCIONES DE LOS PRINCIPALES ROLES DE TI

Las funciones del **Secretario Técnico** son:

- Asesorar en la prioridad de ejecución de actividades y proyectos relacionados con TI de la entidad educativa.
- Coordinar y consolidar la elaboración del Plan Operativo Anual del ámbito de la Secretaría Técnica de Tecnologías de la Información, con las Direcciones Técnicas de Sede, Coordinación de Desarrollo de Software, Coordinación de Infraestructura y Redes y demás dependencias de la Universidad.
- Definir y actualizar conjuntamente con las Direcciones Técnicas de Sede y Coordinaciones, las políticas y procedimientos de tecnologías de información
- Supervisar el cumplimiento de políticas y procedimientos definidos por la institución en el área de TI.
- Formular los programas y planes (Proyectos) de acción para ejecutar las políticas y directrices, conjuntamente con las Direcciones Técnicas de Sede, Coordinación de Desarrollo del Software y Coordinación de Infraestructura y Redes.
- Participar en la planificación de la arquitectura de Hardware y Software conjuntamente con las Direcciones Técnicas de Sede y Coordinación de Infraestructura y Redes.

- Participar en la planificación de las seguridades físicas y lógicas de los sistemas informáticos, evaluación de riesgos y elaboración de planes de contingencia y aceptación de riesgos.
- Supervisar la operatividad de los sistemas y servicios informáticos.
- Supervisar las actividades destinadas a mantener un adecuado control de los activos destinados al área de Tecnología de la Informática.
- Asesorar en las adquisiciones de hardware y software para la Universidad.

Las funciones del **Director de Sistemas** son:

- Elaborar el plan operativo del área de TI.
- Garantizar una disponibilidad del 99.9 % en los servicios de TI que brinda la Universidad.
- Custodiar los dispositivos de respaldo.
- Optimizar el uso de los recursos informáticos.
- Coordinar con la Secretaría Técnica de TI las adquisiciones de hardware y software para la Universidad.
- Cumplir y hacer cumplir la normativa emitida en cuanto a los ámbitos de TI.
- Presentar al Rector de la Universidad el plan operativo y la planificación informática del área de su responsabilidad para su aprobación.

Las funciones del **Administrador de la Base de Datos** son:

- Garantizar la seguridad del sistema de base de datos.
- Instalación de nuevos componentes de software de base de datos.
- Monitorear el rendimiento de la base de datos.
- Realizar procesos de respaldo y recuperación en base a los procedimientos establecidos.
- Afinar la base de datos con el soporte de proveedores.
- Apoyar en el diseño de estructuras de base de datos.
- Analizar datos y realizar recomendaciones concernientes a mejorar el rendimiento y la eficiencia en el manejo de los datos.
- Asistir a los desarrolladores en el afinamiento de sentencias SQL y construcción de procedimientos almacenados.
- Apoyar en la definición de estándares de diseño

Las funciones del **Administrador de Infraestructura** son:

- Planificar la infraestructura tecnológica de la entidad educativa en coordinación con las Direcciones Técnicas de las sedes.
- Elaborar el presupuesto de la infraestructura Tecnológica y Redes de la UPS en coordinación con las Direcciones Técnicas de las sedes.

- Formular, proponer mejoras y supervisar el cumplimiento de políticas y procedimientos de seguridad informática, respaldo, replicación y restauración de información.
- Elaborar especificaciones técnicas de procesos de selección de servicios y equipamiento relacionados con la infraestructura de telecomunicaciones, servidores.
- Supervisar el cumplimiento de las especificaciones eléctricas en la infraestructura informática.
- Administrar los servicios de Internet, correo electrónico, datos, video conferencia (Red convergente) y telefonía IP de la Universidad (administración de usuarios, servidores, dispositivos de comunicaciones y otros).
- Supervisar las actividades relacionadas con los servidores, bases de datos, networking y licencias de software de la Universidad.
- Administrar el inventario de estructura de telecomunicaciones, hardware y software.
- Mantenimiento de la infraestructura tecnológica, equipos de cómputo, equipos de comunicación, sistemas de video conferencia, sistemas de telefonía IP y servicios.
- Elaborar los planes de mantenimiento preventivo, correctivo y de contingencia de la infraestructura tecnológica y Redes.
- Supervisar el cumplimiento de los Planes de mantenimiento..

- Supervisar el uso de los servicios de la Red informática.
- Mantener actualizada la información relacionada a la infraestructura tecnológica de la UPS (Planimetría).
- Mantener operativos los servicios de aplicaciones corporativas de redes y servidores.
- Monitoreo, supervisión y gestión de alertas de servicios de redes, servidores y sistema eléctrico.
- Elaborar la evaluación de riesgos y los planes de contingencia de la UPS en los ámbitos de los servicios de telecomunicaciones.

POLITICAS Y PROCEDIMIENTOS DE TI

Las políticas, planes, estándares para el área de TI son definidas en la sede principal y adoptadas por todas las sedes.

A nivel de políticas la entidad maneja la Política de Respaldos de Información y la política de servicios informáticos.

La política de Respaldos detalla cómo se deben de manejar los mismos, mayor detalle de la política ver en la sección de Backups de este documento.

La política de servicios informáticos, es una política de seguridad orientada a los usuarios que indica los lineamientos que se deben considerar para los mismos sobre los principales recursos proporcionados

Existe además el plan de Mantenimiento de Infraestructura, estándares para programación web, y un estándar para la documentación de políticas, procedimientos y estándares que se definen dentro del área de sistemas.

PROYECTOS DE TI

El área de TI actualmente tiene los siguientes proyectos:

- Proceso de implementación de su plan de contingencia a nivel nacional
- Proceso de virtualización de servidores
- Could de Correos
- Migración servidores de Base de Datos Oracle a una nueva versión 11 a 11.2.

MANEJO DEL RIESGO DE TI

DEPENDENCIA DE TI

Se puede identificar una alta dependencia de los servicios de tecnología en lo referente a las capacitaciones virtuales.

Los sistemas de académicos y financieros tienen su demanda pero en fechas puntuales que no interrumpen la continuidad del negocio.

CONOCIMIENTOS Y RECURSOS DE TI

El personal IT de la compañía mantiene conocimiento sobre toda la gestión que realiza el área entre las principales tenemos:

- ✓ Configuración y Mantenimiento de equipos servidores
- ✓ Mantenimiento de Redes
- ✓ Mantenimiento de cambios sobre los sistemas
- ✓ Soporte a Usuario sobre los sistemas

TI EXTERNO

El área de TI, tiene actualmente el servicio de consultas y mantenimiento preventivo de la base Oracle.

Adicionalmente se tiene una empresa que se encarga del desarrollo de cambios y nuevos requerimientos de una aplicación puntual, debido a la demanda.

AUDITORIA INTERNA

La entidad educativa no registra auditorías internas ya que no cuenta con el personal para la ejecución de la misma, esporádicamente se realizan auditorias puntuales por temas de tesis.

En el año 2010 se realizó una auditoría externa contratada.

INFRAESTRUCTURA DE TI

Existe un plan de mantenimiento sobre la infraestructura de TI (servidores, red u otros componentes) que considera el mantenimiento preventivo y/o correctivo sus responsables y frecuencia de los mismos.

Detalle de la infraestructura principal de la entidad educativa:

SOFTWARE

La entidad educativa cuenta con varias plataformas en las cuales se encuentran instaladas las aplicaciones que le permite soportar sus actividades: financieras, operativas y educativas. Es así que cuenta con las siguientes aplicaciones:

- ✓ El aplicativo central, financiero que fue adquirido con fuentes y actualmente realizan sus modificaciones y se encuentra sobre una base de datos ORACLE.
- ✓ El sistema académico SNA que se encuentra sobre una base de Oracle.
- ✓ El sistema que soporta el servicio de telefonía de la entidad educativa y que tiene como base de datos SQL, este sistema es a nivel nacional.

- ✓ El sistema de la plataforma virtual que permite la administración de las capacitaciones en línea y la publicación de Tesis, este sistema tiene como base de datos Postgres y es a nivel nacional.

HARDWARE

La infraestructura que soporta todos los servicios que presta el área de TI a las sedes educativas se encuentra centralizada en CUENCA, donde están los servidores centrales y en cada una de las sedes se encuentran servidores que sirven de FILE SERVER.

La sede de cuenca cuenta aproximadamente con 40 servidores en total.

- ✓ Plataforma IBM,
- ✓ 2 racks
- ✓ 1 servidor de aplicaciones,
- ✓ IBM 510, que se utiliza para el desarrollo de las aplicaciones
- ✓ IBM 550

Los servidores que actualmente son parte de la infraestructura tecnológica tienen varios sistemas operativos:

- ✓ AIX-Linux
- ✓ CENTOS 5.5
- ✓ ReHat
- ✓ Win 2003-2008

Existe un proyecto para implementar a futuro virtualización de los servidores.

Los enlaces de comunicaciones con los que se realiza la comunicación son dedicados y provistos por TELCONET.

Para el monitoreo de los servidores se usa una herramienta CACTI, que permite revisar las siguientes características:

- ✓ Enlaces
- ✓ Particiones de disco duro
- ✓ Memoria
- ✓ Procesador

BASE DE DATOS

La entidad educativa actualmente cuenta con 4 tipos de bases de datos donde almacenan los datos de varios de sus sistemas informáticos y son:

- ✓ Oracle 11g
- ✓ SQL
- ✓ Postgres
- ✓ MySql

La base Oracle en donde se almacenan los datos de su aplicativo central, financiero y académico.

La base SQL almacena los datos del sistema de telefonía con el que cuenta la entidad educativa a nivel nacional.

La base Postgres almacena la información de las distintas publicaciones que realiza la entidad educativa.

La base MySql soporta la aplicación que permite a la entidad educativa dar el servicio de educación virtual o en línea.

ENTENDIMIENTO DE CONTROLES DE TI

GESTIÓN DE LA SEGURIDAD DE TI

SEGURIDAD FÍSICA Y CONTROL AMBIENTAL

La seguridad implementada a nivel físico en el centro de cómputo es mediante tarjetas de aproximación, mediante la cual se restringe el acceso al mismo. Actualmente las tarjetas que permiten el ingreso se encuentran autorizadas a:

- ✓ Coordinador de sistemas
- ✓ Coordinador de Infraestructura

El data center cuenta con los siguientes controles para su operación:

- ✓ Alarmas contra incendio
- ✓ Medidores de humedad
- ✓ Climatizadores
- ✓ Piso falso
- ✓ Control de ingreso mediante tarjeta de aproximación
- ✓ Cámaras

- ✓ Personas autorizadas al ingreso las que se definen Secretario Técnico, Director de sistemas, Administrador de Infraestructura.
- ✓ Notificaciones vía correo o SMS sobre irregularidades detectadas en el centro de cómputo por medio de alarmas.

Adicionalmente como respaldo en la parte eléctrica cuentan con una planta alterna que permite su operación en caso de corte del fluido eléctrico.

Es importante mencionar que no se ha establecido pruebas de dichos controles.

Las sedes cuenta con un data center donde se encuentran los servidores de archivos y dominios que lo administra cada sede y que se consolida en la sede principal de Cuenca.

SEGURIDAD LÓGICA

Las configuraciones de los firewall, son administradas por el coordinador de infraestructura, teniendo como control de acceso a que solo la IP de la máquina de esta persona está autorizada al ingreso de las mismas.

Firewall: Existe un firewall instalado en cada servidor que es administrado únicamente por el administrador de redes y comunicaciones.

Control de acceso lógico

A nivel de Usuarios de Red

Existen definidos Grupos definidos dentro del Active Directory por cada ciudad y GPO definidas por ciudades.

El acceso a cada uno de los equipos que forman parte de la infraestructura tecnológica se centralizan en un servidor de Active Directory a nivel nacional.

A nivel de Aplicativos

A nivel del Aplicativo Portal Web existe un sistema de autenticación única, la contraseñas es mínimo de ocho caracteres y debe incluir mayúsculas y minúsculas, además que existe un estándar definido para la creación de los identificadores de usuarios.

A nivel de Base de Datos

El acceso a las bases de datos es autorizado mediante correo electrónico del director de sistemas o de desarrollo. Los directores de soporte de cada una de las sedes notifican al director de la sede Cuenca.

Una vez autorizada dicha solicitud es remitida al DBA el cual ejecuta la creación del usuario.

Adicionalmente a nivel de base de datos existen usuarios que son utilizados por proveedores externos durante el proceso de mantenimiento preventivo en la base de Oracle, estos usuarios según se indica son desactivados de forma manual una vez culminada la actividad.

A la fecha de corte del presente informe se tiene como ultimo mantenimiento registrado el 24 de julio del 2011.

GESTIÓN DE USUARIOS

Es importante indicar que por cada usuario que se crea en el sistema financiero y en el SNA, se creará un usuario de la base de datos y los dos manejan la misma clave. Esta clave según lo indicado se encuentran encriptadas en la base mediante una funcionalidad de la misma; el nivel de encriptamiento es DES.

En caso de intentos fallidos el usuario será bloqueado por un periodo de una hora, posterior a este se activará automáticamente.

El registro de los accesos y bloqueos de clave se registran en los logs que son revisados por el dba. El resultado de dicha revisión no genera informe alguno a menos que este sea solicitado.

El registro de la creación de estos usuarios no se documenta mediante documentos estándares formales sino en registros propios del dba, en donde adicionalmente se registran los roles existente.

Para el proceso de baja de usuarios actualmente se realiza bajo la siguiente modalidad:

GTH (Gestión del talento Humano) comunica bajo solicitud de sistemas los usuarios que han dejado de laborar en la institución, esta notificación no se realiza de manera oportuna.

Cuando se ha identificado un usuario que ha dejado de laborar el proceso a seguir es realizar el bloqueo de dicho usuario por un periodo de una semana.

GESTIÓN DE LAS OPERACIONES DE TI

GESTIÓN DE BACKUPS

La gestión de Backups se encuentra respaldada por la Política de RespalDOS de Información que actualmente la empresa tiene aprobada con Versión 1 y fecha de aprobación a Agosto del 2010.

El alcance de dicha política es a toda la información que se almacena en los servidores de la entidad educativa, quedando fuera de esta la información de los equipos personales de los usuarios.

Se identifica como propietario de dicho proceso al Secretario Técnico siendo el responsable de:

- ✓ Establecer las medidas de seguridad necesarias para garantizar el adecuado almacenamiento del presente documento.
- ✓ Definir los perfiles que tendrán acceso al documento.
- ✓ Asegurar la accesibilidad del documento para quienes necesiten consultarlo.
- ✓ Comunicar la existencia del documento y asesorar sobre el mismo a los responsables de su cumplimiento.
- ✓ Solicitar actualizaciones fuera del esquema normal.
- ✓ Actualización de la política con una frecuencia semestral ó bajo demanda.

Se identifica como ejecutantes del proceso al Director de Sistemas y los Directores de Soporte y mantenimiento, adicionalmente son responsables de los traslados de las cintas de respaldos fuera de la entidad educativa.

Para determinar el tipo de respaldo que se realiza a la información se lleva un registro con la siguiente información:

- ✓ Tipo de información.
- ✓ Dueño de la información.
- ✓ Requisitos para ser respaldada la información. (Los requisitos de respaldo pueden ser, por ejemplo, asegurar la recuperación de la información del día anterior, la necesidad de guardar copias de respaldo históricos por un determinado período, etc.)
- ✓ Observaciones.

Los respaldos de los distintos equipos servidores se ejecutan mediante la herramienta Tivoli Store la cual se programa y cumple con las frecuencias que requiere cada equipo de acuerdo a las políticas establecidas.

La frecuencia de respaldos es:

- ✓ Diaria para la información de los usuarios.
- ✓ Diaria para las bases de datos incremental.
- ✓ Semanalmente total las bases de datos, , generalmente el siguiente día hábil.

- ✓ Mensualmente se realizan los respaldos totales de cada uno de los servidores, generalmente el siguiente día hábil
- ✓ Semanalmente se respalda las configuraciones del servidor de aplicaciones de Oracle, donde los datos a ser respaldados son el Application Server.
- ✓ ANUAL: el respaldo se realiza una vez al año, generalmente el siguiente día hábil.
- ✓ OTROS: destinado al tipo de información que requiere ser resguardada y que no aplique ninguno de los esquemas de periodicidad anteriores.

Los tipos de respaldos sobre la información son:

- ✓ COMPLETO: se resguarda toda la información
- ✓ INCREMENTAL: se resguarda la información que se haya incorporado desde el último respaldo realizado
- ✓ DIFERENCIAL: se resguarda sólo la información que se haya modificado desde el último respaldo realizado.

La rotación de las cintas determina el criterio bajo el cual se reutilizarán los dispositivos físicos de respaldo estableciendo como máximo el recomendado por el fabricante lo cual

se encuentra determinado en la política y el registro de la vigencia de dichos dispositivos son reflejados en una bitácora de datos.

Los dispositivos que deban ser desechados serán eliminados de manera segura garantizando la imposibilidad de que la información ahí almacenada pueda ser leída.

Se identifica como dispositivos válidos para ser usados como destino de respaldo cinta magnética o disco para las localidades que no tengan el lector de cintas.

Los respaldos anuales, mensuales, y semanales serán almacenados fuera de las instalaciones de la entidad educativa, y estar disponibles en el momento que se requiera.

El registro de la ejecución de cada una de las tareas realizadas para backups, se registran en el log de la aplicación que realiza esta actividad. La revisión de esta información es del coordinador de infraestructura quien también autoriza la ejecución de las mismas.

En base a la frecuencia de los respaldos se establece lo siguiente:

- ✓ Pérdida de información, la que haya sido registrada en 5 minutos.
- ✓ Tiempo de recuperación del servidor de las aplicaciones financieras y SNA
3 horas.

Es importante mencionar que no se informa sobre actividades de prueba para el cumplimiento de los tiempos indicados.

El proceso de verificación de los respaldos realizados se realiza de la siguiente manera:

- ✓ Semanalmente se restaurará una copia diaria realizada.
- ✓ Trimestralmente se restaurará la última copia mensual realizada.

La recuperación se realizará en un ambiente de prueba para evitar que dicho proceso afecte al ambiente de producción. El resultado de dicho proceso se registra en una bitácora.

Adicionalmente se respaldan los logs de las bases, dichos respaldos son conservados por un periodo de 6 meses.

GESTIÓN DE INCIDENCIAS

La gestión de los incidentes que se presentan en ambientes de producción son resueltos por el coordinador de sistemas como soporte de primer nivel, en caso de requerir una revisión más detallada se solicita la intervención del área de sistemas.

PLAN DE CONTINGENCIA

Actualmente se encuentran en un proceso e implementación de un DRP con la finalidad de contar con las políticas y procedimientos necesarios para asegurar la funcionalidad y recuperación del área de TI a nivel nacional.

GESTIÓN DE OPERACIONES Y CONFIGURACIONES

Las configuraciones de los servidores y equipos principales se respaldan durante el proceso de respaldos. Únicamente el administrador de redes y comunicaciones es el encargado de administrar estas configuraciones

GESTIÓN DE CAMBIOS A PROGRAMAS

Para la gestión de cambios a los aplicativos actuales se realiza bajo demanda operativa donde se presenta la solicitud al director de sistemas, bajo el levantamiento de la parte usuario en documentos no formales que registran el alcance de los cambios a realizarse en las aplicaciones.

Este levantamiento es sometido al secretario técnico quien finalmente realiza la aprobación o no de lo solicitado.

GESTIÓN DE DERROLLO DE SISTEMAS

La entidad educativa cuenta con un documento formal en donde se establecen los estándares bajo los cuales se realizan los desarrollos de los sistemas web.

El objetivo del estándar es facilitar el desarrollo de las aplicaciones, se establece como dueño del proceso al director de Sistemas, cuyas responsabilidades son:

- Establecer los estándares de programación para futuras aplicaciones web.
- Asegurar la accesibilidad del documento para quienes requieran consultarlo.
- Comunicar la existencia del documento y asesorar sobre el mismo a los responsables de su cumplimiento.
- Solicitar actualizaciones fuera del esquema normal.

Los ejecutantes de todos los desarrolladores.

Las versiones que se salen a producción en lo referente a las aplicaciones que se desarrollan internamente no registran documentación formal.

Para el caso de versionamiento de software tampoco existe la documentación formal de cambio realizado salvo casos aislados que mantienen un registro de las actualizaciones que se realizan.

EVALUACIÓN DE ESTRUCTURA DE RIESGOS/ CONTROLES

SIGNIFICADO DE LA EVALUACIÓN DE RIESGOS

Es el proceso de identificar y analizar las amenazas sobre el ambiente de control interno, que está asociada con las prácticas financieras estratégicas y tácticas y con las prácticas operacionales de IT, las cuales pueden afectar la capacidad de la organización para alcanzar sus objetivos.

El propósito de realizar esta evaluación es, en primer lugar identificar los riesgos que afectan a la organización, evaluar la probabilidad y el potencial impacto que estos riesgos podrían y definir e implementar controles apropiados para en forma efectiva, reducir, eliminar y administrar el impacto asociado con esos riesgos.

ESTRUCTURA DE LA EVALUACIÓN DE RIESGOS

Para evaluar la estructura de controles existentes dentro de la entidad educativa utilizaremos un enfoque que nos proporcionan las mejores prácticas para la evaluación de

riesgos e identificación de controles asociados, para lo cual hemos definido por cada dominio de los controles la ejecución de los siguientes pasos:

- Identificar los subprocesos del proceso de facturación
- Identificar las actividades que conforman cada subproceso
- Identificar los objetivos de Control de cada actividad
- Identificar los riesgos asociados a los objetivos de control identificados
- Establecer la exposición al riesgo de cada actividad
- Identificar los controles actuantes relacionados a cada riesgo
- Evalúa el control en su diseño
- Determina la efectividad del control en función de pruebas de auditoria
- Identifica oportunidades de mejora a ser reportadas.

El enfoque considerado nos proporciona de forma integral un análisis y evaluación sobre los riesgos y controles del proceso.

Como resultado podremos considerar que estaremos analizando:

- Alineación con los objetivos de la organización.
- Identificación de la exposición a amenazas y vulnerabilidades del proceso analizado
- Identificación y valoración de los riesgos asociados

- Evaluación de los controles existentes y su efectividad para el logro del objetivo de control.

CLASIFICACIÓN DE LOS RIESGOS

La clasificación de los riesgos para cada evento identificado, se la realizará considerando la criticidad de los puntos en cuestión de la Gestión del Proceso de Facturación y el ambiente de Gestión de TI que lo soporta: esta calificación estará dada por el criterio profesional del equipo asignado

1	Riesgo Bajo. Evento menor a ser considerado. Impacto mínimo en la consecución el objetivo
2	Riesgo Medio. Significativo. Impacto medio en la consecución del objetivo
3	Riesgo alto. Severo. Impacto alto la consecución el objetivo

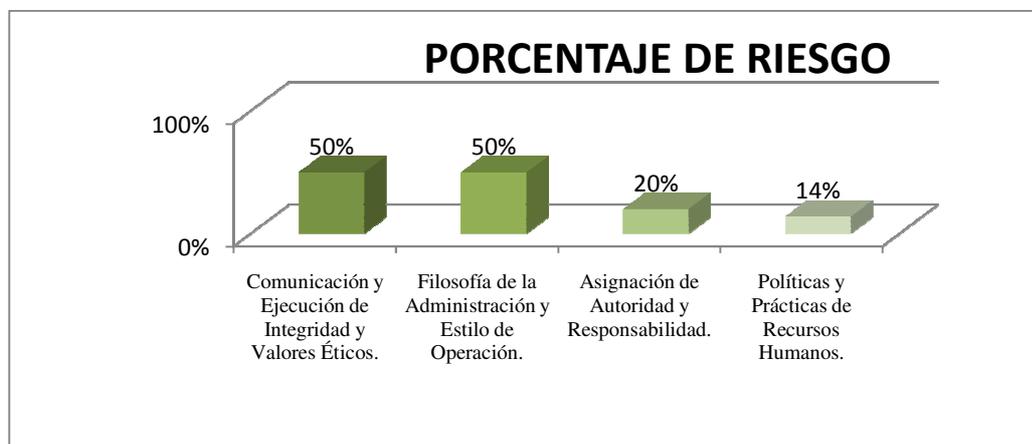
Este proceso se verá reflejado en una Matriz de Riesgos que completará de forma dinámica durante el proceso a medida que avance la evaluación, debido a que en cada

fase de este flujo se irán identificando riesgos asociados deficiencias de controles dentro de la entidad educativa.

EVALUACION DE RIESGOS CONTROL INTERNO

Resultados % de Riesgo:

FACTOR DE RIESGO	PORCENTAJE DE RIESGO
Comunicación y Ejecución de Integridad y Valores Éticos.	50%
Proceso de Gobernabilidad (Junta Directiva y Comité de Auditoría).	0%
Filosofía de la Administración y Estilo de Operación.	50%
Estructura Organizacional.	0%
Compromiso para la Competencia.	0%
Asignación de Autoridad y Responsabilidad.	20%
Políticas y Prácticas de Recursos Humanos.	14%



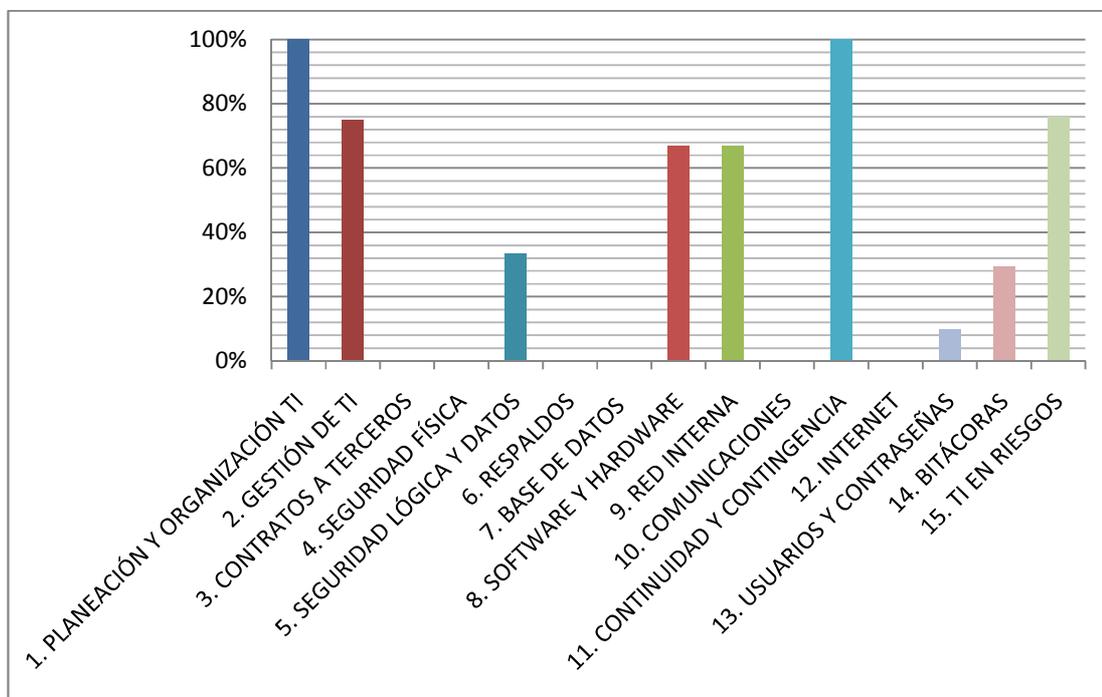
En base a nuestra comprensión y evaluación de Riesgos del Marco de Control Interno determinamos un enfoque de no confort en controles de TI, no obstante el control interno en cuanto al ambiente sobre el cual opera la institución no presenta aspectos relevantes que observar.

Ver detalle: ANEXO I: EVALUACIÓN DE AMBIENTE DE CONTROL DEL PROCESO DE FACTURACIÓN

EVALUACION DE RIESGOS EN TI.

Resultados:

FACTORES DE RIESGO	GRADO DE RIESGO (1% - 100%)
1. PLANEACIÓN Y ORGANIZACIÓN TI	100,00%
1.1. Plan Estratégico de TI	100,00%
1.2. Organización y Relaciones de TI	0,00%
2. GESTIÓN DE TI	75,00%
3. CONTRATOS A TERCEROS	0,00%
4. SEGURIDAD FÍSICA	0,00%
5. SEGURIDAD LÓGICA Y DATOS	33,33%
6. RESPALDOS	0,00%
7. BASE DE DATOS	0,00%
8. SOFTWARE Y HARDWARE	66,67%
9. RED INTERNA	66,67%
10. COMUNICACIONES	0,00%
11. CONTINUIDAD Y CONTINGENCIA	100,00%
12. INTERNET	0,00%
13. USUARIOS Y CONTRASEÑAS	10,00%
14. BITÁCORAS	29,17%
14.1. Sistemas de Información	25,00%
14.2. Red Interna	33,33%
14.3. Comunicaciones	0,00%
15. TI EN RIESGOS	76,00%
15.1. Ajustes	100,00%
15.2. Suministro de Información	0,00%
15.3. Integridad de los sistemas y herramientas de auditoría	40,00%



CONCLUSIONES DE LA EVALUACION DE RIESGOS.

En base al entendimiento y análisis de riesgos sobre el ambiente tecnológico podemos concluir que la entidad educativa desarrolla sus actividades en un ambiente de TI tiene debilidades en controles claves que no nos permite confiar en un ambiente de control tecnológico por lo que sugerimos un enfoque que NO CONFORT EN CONTROLES.

Ver detalle: ANEXO II: MATRIZ DE RIESGO DE TI

IDENTIFICACIÓN DE CONTROL

CONTROLES								
SUB PROCESO	CONTROL	OBJETIVO PROCESAMIENTO DE INF.				D DETECTIVO P PREVENTIVO	FRECUENCIA	TIPO
		I	P	V	R			
Categorización de Estudiantes	Asignación de quintiles a estudiantes de forma automática para determinar valores por créditos en base a su situación económica.	X				P	Semestral	Automático
Descuentos	Valores paramétricos administrados por perfiles, que determinan el valor que es considerado como subsidio del gobierno	X			X	P	Semestral	Automático
Pre-Facturación	Notificación que el estudiante no puede ser registrado, ya que no tiene asignado su categoría, según el análisis de situación económica.	X				P	Semestral	Automático
	Cálculo automático de valores en base a clasificación y categorización automática de los estudiantes	X				P	Semestral	Automático
	Generación automática y secuencial de código de pre-factura.	X				P	Continuo	Automático
	Control de modificación del archivo de cobro para las instituciones financieras.				X	P	Mensual	Manual
Generación de Convenios de Pago	Aprobación de convenio	X	X			P	Semestral	Manual
Liberación de Cupos	Por monto total de pago o convenio aprobado, declara cupo reservado	X	X			P	Continuo	Automático

CONTROLES								
SUB PROCESO	CONTROL	OBJETIVO PROCESAMIENTO DE INF.				D DETECTIVO P PREVENTIVO	FRECUENCIA	TIPO
		I	P	V	R			
Facturación	Carga del archivo de pagos recibidos, validados por cédula del estudiante	X				P	Diario	Automático
	Generación automática de facturas de los estudiantes que han cancelado el monto total facturado.	X				P	Diario	Automático
	Conciliación Bancaria	X	X	X		D	Mensual	Automático
	Cuadre de valores cargados en cuenta bancaria, se realiza la sumatoria de los valores que se detallan en el archivo de los pagos recibidos en cada uno de los bancos vs los movimientos del día en el banco.	X	X			D	Diario	Manual

NOMENCLATURA

OBJETIVOS DE PROCESAMIENTO DE INFORMACIÓN	
Integridad I	Todas las transacciones que se producen se registran y aceptado para el procesamiento de una sola vez y en el período adecuado. Por ejemplo, la duplicación de entradas se identifican y se rechazó, todas las excepciones / rechazos son abordados y resueltos.
Precisión P	Las transacciones se registran por el importe correcto en la cuenta correspondiente y el período adecuado (la entrada de la fecha era correcta) Esto incluye la precisión de los elementos de datos clave y los datos permanentes usados en el procesamiento de transacciones
Validez V	Sólo las transacciones autorizadas que realmente ocurrió y están relacionados con la organización se registran
Acceso restringido R	Los datos están protegidos contra modificaciones no autorizadas y el acceso a los datos confidenciales y los activos físicos es apropiado, restringido a personal autorizado. Puede ser difícil de lograr los otros tres objetivos procesamiento de la información (integridad, exactitud y validez), cuando el objetivo de acceso restringido no se cumple

PROGRAMA DE AUDITORÍA INFORMÁTICA DE LA ENTIDAD EDUCATIVA

El programa de auditoría informática determina el alcance, objetivos y procedimientos de auditoría necesarios para lograr evidencia suficiente, competente y confiable para obtener y sustentar las conclusiones y opiniones de este proceso de auditoría.

OBJETIVO

El objetivo de la auditoría se centra en establecer los controles implementados en el proceso de facturación, además determinar si el ambiente de tecnología en el cual soporta la institución sus procesos protege de manera apropiada los recursos de TI.

ALCANCE

El alcance de la auditoría se define en base a la evaluación del área de tecnología y el proceso de facturación que se ejecuta sobre la misma.

Determinar nuestras observaciones y conclusiones sobre la situación actual del entorno de tecnología de la entidad educativa, nivel de riesgos y controles que se encuentren asociados a los mismos.

Se ha determinado que los dominios de control de TI bajo los cuales se realizó la revisión de los controles son:

- Seguridad Lógica: Acceso a Programas y Datos
- Administración de Desarrollo de sistemas: Cambios a Programas
- Operaciones

Evaluated el ambiente de TI, se emitirá una conclusión sobre el mismo y se procederá a la revisión de controles del proceso de facturación.

Como resultado se entregara un informe final en el que se incluirán las debidas observaciones identificadas con su impacto y recomendaciones para contribuir con las mejoras del control interno en el proceso de facturación.

METODOLOGÍA

Como parte de la estrategia se utilizará como marco de trabajo metodologías tales como:

- NEA

- ISACA.
- ISO 9001-2008
- COBIT V 4.1:
- ITIL V3
- COSO ERM
- Ley Sarbanes-Oxley (SOX)

Estas metodologías nos apoyarán para la ejecución de un trabajo con eficacia y que nos permitan identificar con exactitud los controles de TI más relevantes para el área de sistemas a ser evaluada.

RESPONSABLES

NOMBRES	CARGO
María Verónica Chávez	Auditora de Sistemas – Líder del Equipo
Catania Játiva Vásquez	Auditora de Sistemas

PROCEDIMIENTOS DE AUDITORIA

Los procedimientos generales que se utilizaran para la ejecución de la auditoria son los siguientes:

- Obtener y documentar el entendimiento del área de tecnología.
- Obtener y documentar el entendimiento del proceso de facturación.
- Realizar la planificación general de la auditoria con su respectivo detalle de actividades.
- Obtener y documentar el entendimiento de las áreas de control de TI y definir el enfoque de nivel de aceptación de controles.
- Determinar satisfacción en el diseño e implementación las actividades de control definidas en el proceso de facturación.
- Evaluar la eficiencia operativa de las actividades de control cuyo diseño es satisfactorio.
- Comunicar el resultado de las pruebas sobre el rendimiento de los controles y determinar el plan de acción con el dueño del proceso y área de tecnología.
- Presentar el informe de auditoría a la alta gerencia de la institución.

PLAN DE AUDITORIA

Las actividades detalladas en el presente plan de auditoría serán ejecutas por las dos personas responsables del mismo.

Lsi. María Verónica Chávez

Ing. Catania Játiva Vásquez

Procedimientos	Actividades
Obtener y documentar el entendimiento del área de tecnología.	<ul style="list-style-type: none"> - Solicitar entrevista con el Jefe de Sistemas para obtener el entendimiento inicial de TI. - Documentar los resultados de la entrevista.
Obtener y documentar el entendimiento del proceso de facturación y el ambiente de control en el cual se ejecuta.	<ul style="list-style-type: none"> - Solicitar entrevista con: <ul style="list-style-type: none"> Contadora de la entidad. Tesorera de la entidad. Representante del departamento de bienestar Estudiantil. - Documentar los resultados de la entrevista.

<p>Realizar la planificación general de la auditoria con su respectivo cronograma de actividades.</p>	<ul style="list-style-type: none"> - Determinar las fases de la auditoria - Definir las actividades por fases - Determinar los responsables y fechas de desarrollo por actividad
<p>Obtener y documentar el entendimiento de las áreas de control y definir las actividades de control a probar.</p>	<ul style="list-style-type: none"> - Preparar cuestionarios por cada área de control. - Solicitar reuniones con el personal clave. - Definir las actividades de control por cada área de auditoria
<p>Determinar satisfacción en el diseño e implementación las actividades de control definidas.</p>	<ul style="list-style-type: none"> - Evaluar y documentar diseño de los controles identificados.
<p>Evaluar la eficiencia operativa de las actividades de control cuyo diseño es satisfactorio.</p>	<ul style="list-style-type: none"> - A partir de los controles cuyo diseño es satisfactorio, determinar por medio de pruebas la eficacia operativa de los controles.
<p>Comunicar el resultado de las pruebas sobre el rendimiento de los controles y determinar el plan de acción al</p>	<ul style="list-style-type: none"> - Elaborar un borrador de Informe a partir de las deficiencias de controles identificadas.

delegado de la entidad educativa.	<ul style="list-style-type: none">- Discutir con el Jefe de Sistemas las observaciones del informe.- Discutir con el dueño el proceso las observaciones del informe.- Añadir las acciones de mitigación presentadas por los responsables de las áreas por cada punto del Informe
Presentar el informe de auditoría al delegado de la institución.	<ul style="list-style-type: none">- Preparar el informe definitivo del proceso de auditoría.- Entregar el informe al delegado la entidad educativa.

EVALUACIÓN DE CONTROLES

En la evaluación de controles verificamos la efectividad operativa de los controles identificados, con el fin de determinar si se encuentran operando como fue diseñado y si la persona que realiza el control tiene la autoridad necesaria para realizar el control de manera efectiva.

NATURALEZA DE LAS PRUEBAS DE CONTROLES

Existen cuatro técnicas básicas se utilizan para probar controles: Indagación, Observación, Inspección y Reformulación.

Se han utilizado la combinación de estas técnicas para probar la aplicación de los controles.

ALCANCE DE LAS PRUEBAS DE CONTROLES

El alcance de las pruebas para lograr un alto nivel de aseguramiento se ha determinado al evaluar la **naturaleza** del control, **frecuencia** de operación e **importancia** del control.

NATURALEZA DE LOS CONTROLES MANUALES Y AUTOMATIZADOS

Las pruebas realizadas sobre los controles manuales han sido más extensivas que las pruebas realizadas sobre los controles automatizados.

De acuerdo a la SOX para la evaluación efectiva de las operaciones determina que para las pruebas a realizarse sobre los controles se debe de considerar lo siguiente:

- **Controles Automáticos:** El testeado de un solo ítem puede ser suficiente teniendo en cuenta los atributos que se presentan dentro del control.
- **Controles Manuales:** Cuando se testea controles manuales, basados en la frecuencia del control, los tamaños de muestras sugeridos son los siguientes:

Pruebas de Controles Manuales		
Frecuencia del control manual	Número de partidas a probar	Factores a considerar al decidir sobre el alcance de nuestras pruebas directas (mientras más alto sea el riesgo = más partidas necesitan probarse)
Anualmente	1	<ul style="list-style-type: none"> • Materialidad o riesgo de error del saldo de la cuenta • Complejidad del control • Importancia del juicio en la operación del control • Riesgo de falla evaluado del control operando efectivamente • Controles que tienen un efecto penetrante en los estados financieros • Importancia del control: <ul style="list-style-type: none"> • Tratar múltiples aseveraciones financieras • Controles de detección de fin de periodo
Trimestralmente	2	
Mensualmente	2 a 5	
Semanalmente	5, 10, 15	
Diariamente	20, 30, 40	
Múltiples Veces al Día	25, 30, 45,60	

Muchas de las pruebas de controles, el tamaño mínimo de las muestras nos ha proporcionado evidencia suficiente para concluir sobre la operación de un control específico, en otros casos, hemos tenido que probar muestras más extensas considerando la naturaleza, frecuencia e importancia del control.

ACTIVIDADES DE CONTROL - RESULTADOS

SUB PROCESO	CONTROL	DESCRIPCION DE LAS PRUEBAS	RESULTADO
Categorización de Estudiantes	Asignación de quintiles a estudiantes de forma automática para determinar valores por créditos en base a su situación económica.	<ol style="list-style-type: none"> 1. Solicitar acceso a la pantalla de parametrización quintiles y verificar la existencia de la definición de las cinco categorías dentro del sistema. 2. Verificar con ayuda del administrador del Sistema los usuarios que tienen acceso a la pantalla de parametrización de quintiles. 	<ol style="list-style-type: none"> 1. Por medio de la Contadora se verifico que se encuentran parametrizados cinco tipos de quintiles dentro del Sistema. 2. Pudimos constatar que el Vicerrector General tiene acceso total a opción y el Contador acceso a consulta. <p>Resultado Satisfactorio</p>
Descuentos	Valores paramétricos administrados por perfiles, que determinan el valor que es considerado como subsidio del gobierno	<ol style="list-style-type: none"> 1. Verificar en la pantalla de parametrización de descuentos de quintiles que se encuentren las parametrizaciones de acuerdo a lo definido en el acuerdo del Gobierno. 2. Verificar con ayuda del administrador del Sistema los usuarios que tienen acceso a la pantalla de parametrización de quintiles. 	<ol style="list-style-type: none"> 1. Por medio de la Contadora verificamos que se encuentren aplicados los descuentos definidos según la resolución del Gobierno. 2. Se verifico que el Vicerrector General tiene acceso total a opción y el Contador acceso a consulta. <p>Resultado Satisfactorio</p>

ACTIVIDADES DE CONTROL – RESULTADOS

SUB PROCESO	CONTROL	DESCRIPCION DE LAS PRUEBAS	RESULTADO
Pre-Facturación	Notificación que el estudiante no puede ser registrado, ya que no tiene asignado su categoría, según el análisis de situación económica.	1. Solicitar por medio de la Pagina Web acceso a la cuenta de un estudiante que tiene asignado quintil no permite continuar con el proceso y viceversa (Estudiantes categorizados y no categorizados).	1. Por medio del Asistente de Sistemas: <ul style="list-style-type: none"> - Se creo un usuario de pruebas. - Se accedió con la cuenta - Se estableció una categoría al estudiante. - Se verifico que podía continuar el proceso de registro. -Se quito la categoría al estudiante. - Se verifico que no podía continuar con el proceso de registro. <p>Resultado Satisfactorio</p>
	Cálculo automático de valores en base a clasificación y categorización automática de los estudiantes	1. Solicitar un ejemplo de factura por cada tipo de quintil y revisar el cálculo la pre-facturas y facturas de estudiantes.	1. Con ayuda de la Tesorera se revisaron una factura por cada quintil y se reviso el cálculo de valores a pagar por los estudiantes. <p>Resultado Satisfactorio</p>

ACTIVIDADES DE CONTROL – RESULTADOS

SUB PROCESO	CONTROL	DESCRIPCION DE LAS PRUEBAS	RESULTADO
Pre-Facturación	Generación automática y secuencial de código de pre-factura.	1. Verificar que en la pantalla de facturación al seleccionar Nueva Factura y verificar la generación automáticamente del número secuencial de la factura.	1. Se verifico la generación del secuencial de factura. Resultado Satisfactorio
	Control de modificación del archivo de cobro para las instituciones financieras.	1. Solicitar al Asistente de Sistemas los usuarios que tienen acceso a la pantalla de generar archivo de cobros. 2. Verificar que el archivo de cobros no pueda ser modificado una vez generado	1. Se verifico que el Gerente Financiero, Contadora y Cajera-Tesorera tienen acceso a generar el archivo de cobros. 2. El archivo generado se deposita en una ruta no protegida, siendo expuesto a modificaciones no autorizadas. Resultado No Satisfactorio

ACTIVIDADES DE CONTROL - RESULTADOS

SUB PROCESO	CONTROL	DESCRIPCION DE LAS PRUEBAS	RESULTADO
Generación de Convenios de Pago	Aprobación de convenio	<ol style="list-style-type: none"> 1. Solicitar la carpeta de convenios. 2. Seleccionar una muestra de 60 convenios (De acuerdo a lo definido por SOX). 3. Revisar que los documentos de convenios cuenten con la firma y sello de aprobación y que los mismos estén registrados en el documento de Excel donde se registran los convenios aprobados. 	<p>Se verifico la aprobación con firma y sello en los documentos y se verifico su registro en el formato de Excel.</p> <p>A pesar de que el proceso se realiza de forma controlada, se recomendará la automatización del mismo.</p> <p>Resultado Satisfactorio</p>

ACTIVIDADES DE CONTROL – RESULTADOS

SUB PROCESO	CONTROL	DESCRIPCION DE LAS PRUEBAS	RESULTADO
Liberación de Cupos	Por monto total de pago o convenio aprobado, declara cupo reservado	1. Verificar por medio del acceso a la cuenta de un estudiante de prueba por modalidad de convenio que el mismo tenga sus cupos se encuentren confirmados.	1. Con la ayuda del Asistente de Sistemas se parametrizó a un usuario de prueba para que tenga modalidad de convenio y verificamos que los cupos se encuentran reservados. Así mismo se definió para que la modalidad sea pago normal y el pago se haya efectuado y verificamos la reserva del cupo. Resultado Satisfactorio

ACTIVIDADES DE CONTROL – RESULTADOS

SUB PROCESO	CONTROL	DESCRIPCION DE LAS PRUEBAS	RESULTADO
Facturación	Carga del archivo de pagos recibidos, validados por cédula del estudiante	<p>1. Verificar por medio del acceso a la cuenta de un estudiante de prueba, a través del sistema de la página web, corroborar del estado del pago del estudiante antes de la carga del archivo.</p> <p>Verificar después de la carga del archivo que el estado del pago cambio. (Pendiente, Cancelado), estado del cupo (pre registrado) y monto.</p>	<p>1. Se verifico previo y después del pago el cambio de estado del pago, estado del cupo y monto.</p> <p>Para el caso de estudiantes que realicen pagos parciales en las ventanillas de las instituciones financieras, el sistema detecta varios pagos con el mismo número de cobro y no permite la carga, para proceder con la misma se actualiza la información de forma manual en el archivo.</p> <p>Resultado Satisfactorio</p>

	Generación automática de facturas de los estudiantes que han cancelado el monto total facturado.	1. Visualizar el proceso del cuadro total del archivo con total de facturas generadas del día.	1. Se comprobó con la Tesorera por medio de la observación el cuadro de la facturación de un día. Resultado Satisfactorio
--	--	--	---

ACTIVIDADES DE CONTROL – RESULTADOS

SUB PROCESO	CONTROL	DESCRIPCION DE LAS PRUEBAS	RESULTADO
Facturación	Conciliación Bancaria	1. Visualizar el proceso Cuadre de valores de cuenta bancaria (archivo de estado de la cuenta) con transacciones generadas en el sistema por concepto de recaudaciones.	1. Se verifico con la Tesorera por medio de la observación la conciliación de los valores de estado de cuenta con el archivo de recaudaciones realizadas del generado del sistema al cierre del mes. Resultado Satisfactorio

	<p>Cuadre de valores cargados en cuenta bancaria, se realiza la sumatoria de los valores que se detallan en el archivo de los pagos recibidos en cada uno de los bancos vs los movimientos del día en el banco.</p>	<p>1. Visualizar cuadro de valores de cuenta bancaria (archivo de movimientos de la cuenta) con transacciones generadas en el sistema por concepto de recaudaciones de un día.</p>	<p>1. Con la ayuda de la Tesorera se verifico el archivo de movimientos de la cuenta con las transacciones por recaudaciones del sistema de un día.</p> <p>Resultado Satisfactorio</p>
--	---	--	---

INFORME

En documento aparte se remite informe resultado de la presente auditoría.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

Durante nuestro proceso de auditoría introducimos la relevancia del control interno del proceso de facturación, que esto involucra a todo el ambiente de control de la institución para lo cual verificamos que se encuentren definidas actividades que aseguren el cumplimiento de las directrices de la institución y emitir recomendaciones al respecto, con lo que se logro cumplir con los objetivos planteados al inicio de la tesis.

El aporte de esta tesis es investigativo y metodológico. Investigativo debido a que se realizo un proceso de recopilación de información sobre el control interno en el proceso evaluado. Metodológico porque se siguieron enfoques sugeridos por mejores prácticas para la elaboración de un proceso de auditoría y para poder generar recomendaciones acordes a estos enfoques, consiguiendo que las mismas atiendan los objetivos de la institución como parte de su control interno.

RECOMENDACIONES:

Es importante destacar que las recomendaciones generadas para la Institución Educativa se encuentran en el Informe de Control Interno del Proceso de Facturación.

Destacamos que es importante que las empresas de nuestro país profundicen en la relevancia que tiene el control interno dentro de sus organizaciones y como este aporta significativamente a sus procesos, con la identificación temprana y administración adecuada de los riesgos. Las mejoras se dan a todo nivel de la organización: Gerencial, administrativo/operativo, y de Soporte.

Adicionalmente deben considerar incluir dentro de sus procesos de control la participación de áreas auditoría que puedan colaborar con un enfoque metodológico que aporte en la mejora de su control interno.

ANEXOS

**ANEXO I: EVALUACIÓN DE AMBIENTE DE CONTROL DEL PROCESO DE
FACTURACIÓN.**

EVALUACIÓN DEL AMBIENTE DE CONTROL ENTIDAD EDUCATIVA						
COMPONENTE	AMBIENTE DE CONTROL					
FACTOR A EVALUAR	ÍTEMS QUE COMPONEN EL FACTOR A EVALUAR	DESCRIPCIÓN DE LAS PRUEBAS A REALIZAR	SI	NO	NO APLICA	
Comunicación y Ejecución de Integridad y Valores Éticos.	1-A. Códigos de Conducta, Comportamiento Ético y Moral.	Se poseen Códigos de Conducta o Reglamento Interno de trabajo que regule las conductas y comportamientos de los empleados de la entidad?	1			
		Se garantiza el entendimiento del código de conducta por parte de los empleados?		1		
		Se requieren confirmaciones periódicas sobre el cumplimiento del Código de conducta a empleados claves?			1	
		Están claramente definidas cuáles podrían ser las consecuencias (acciones disciplinarias) de actos indebidos por parte de los ejecutivos y otros empleados de la Entidad?	1			
	1-B. Prácticas de Negocio Aceptables	Se poseen políticas que regulen las prácticas de negocio aceptables?	1			
		Se asegura que el comportamiento ético sea considerado cuando se trata con grupos de interés (Accionistas, proveedores, clientes, auditores, entre otros)?	1			
		Se documentan las decisiones de "excepciones" a políticas/prácticas de recursos humanos de la compañía por parte de la alta gerencia?			1	
	1-C. Conflictos de interés	Se poseen políticas que regulen los conflictos de interés?	1			
	1-D. Relaciones con empleados, proveedores, competidores, entes de control, inversionistas	Se poseen políticas que regulen situaciones como: -Relaciones entre empleados? - Relaciones con proveedores? -Relaciones con los Competidores? - Relaciones con los Entes de Control?	1			
	1-E. Incentivos y Tentaciones	Se ha evidenciado una inadecuada segregación de funciones en áreas sensibles que ofrecen facilidad para robos o para cubrir malos desempeños?			1	
		Se ha evidenciado una alta descentralización de controles que evidencie una inadecuada administración?			1	
		Se ha evidenciado una inadecuada administración que no proporciona advertencia a las negligencias?			1	
		Los reconocimientos y promociones son exclusivamente por logros y desempeño?	1			
		Se ha evidenciado que las sanciones impuestas son insignificantes y no son publicadas o dadas a conocer a toda la Entidad?			1	
				50%	50%	

EVALUACIÓN DEL AMBIENTE DE CONTROL ENTIDAD EDUCATIVA					
COMPONENTE	AMBIENTE DE CONTROL				
FACTOR A EVALUAR	ÍTEMES QUE COMPONEN EL FACTOR A EVALUAR	DESCRIPCIÓN DE LAS PRUEBAS A REALIZAR	SI	NO	NO APLICA
Proceso de Gobernabilidad (Junta Directiva y Comité de Auditoría).	2-A. Independencia frente a la Administración	Existe un plan estategico de la Entidad?	1		
		En caso de existir, ese plan es difundido a toda la organización?	1		
	2-B. Frecuencia y oportunidad de las reuniones de la JD y el Comité	Se posee la adecuada frecuencia y oportunidad de las ejecuciones de las reuniones con el primer nivel administrativo?	1		
	2-D. Suficiencia y oportunidad de la información que se somete a evaluación	Existe adecuada suficiencia y oportunidad en el monitoreo del cumplimiento de los objetivos y estrategias de la Entidad?	1		
Existe adecuada suficiencia y oportunidad en la información sensitiva e investigaciones de actos impropios (Ejemplo: Gastos de viajes de ejecutivos principales irregulares, litigios significativos, uso indebido de activos, desfalco, peculado y cualquier violación de las reglas del negocio)?		1			
			100%	0%	
Filosofía de la Administración y Estilo de Operación.	3-A. Naturaleza de los riesgos de negocios aceptados	Se cuenta con una política de Administración de Riesgos?		1	
		Se evalúan los riesgos y algunos de ellos son aceptados por la administración (Asumidos)?		1	
	3-B. Interacción entre la dirección general y la parte operativa	Se manifiesta el interés de la Dirección de la Entidad con el sistema de Control Interno a través de reuniones, conferencias internas, cursos y otros medios que permita percibir a toda la organización el compromiso de la alta Dirección con el sistema de control interno?	1		
	3-C. Actitudes y acciones frente a la información financiera	Se evalúan las actitudes y acciones frente a la información financiera, incluyendo posiciones frente a la aplicación de acuerdos contables (Las políticas contables son conservadoras o liberales, principios contables han sido erradamente aplicados, no se revela información financiera importante, se manipulan o falsifican los registros) ?	1		
3-D. Actitudes y acciones hacia el procesamiento de datos y funciones de contabilidad y personal					

EVALUACIÓN DEL AMBIENTE DE CONTROL ENTIDAD EDUCATIVA					
COMPONENTE	AMBIENTE DE CONTROL				
FACTOR A EVALUAR	ÍTEMES QUE COMPONEN EL FACTOR A EVALUAR	DESCRIPCIÓN DE LAS PRUEBAS A REALIZAR	SI	NO	NO APLICA
Estructura Organizacional.	4-A. Definición de áreas claves de autoridad y Establecimiento de líneas apropiadas de información	Cuenta la entidad con una estructura organizativa que manifieste claramente las relaciones jerárquico/funcionales de la organización y permita el flujo de información entre las áreas?	1		
		Está difundido a toda la organización?	1		
		La estructura prevista es adecuada al tamaño y naturaleza de las operaciones?	1		
		Se poseen claramente definidas las responsabilidades claves de los administradores?	1		
	4-B. Claridad en el conocimiento y experiencia de los administradores a la luz de sus responsabilidades	Se posee como buena practica la divulgación de las responsabilidades definidas en los cargos o algún mecanismo de consulta permanente?	1		
		Cuenta su área con el personal suficiente y capacitado para cumplir con los objetivos definidos?	1		
		Se evalúa el conocimiento y experiencia de los administradores claves, a la luz de sus responsabilidades (Ejemplo: Evaluaciones de desempeño)?	1		
			100%	0%	
Compromiso para la Competencia.	5-A. Descripciones formales o informales del trabajo	Han sido claramente definidos y comunicados los manuales de funciones y cargos para el personal (descripción de cargos)?	1		
		Dichas descripciones de cargos especifican el nivel de conocimiento y habilidades que se requiere de dicho personal?	1		
	5-B. Requisitos de conocimiento y habilidades para el talento humano	El desempeño del personal "supervisor" es evaluado periódicamente, considerando los aspectos mencionados en las descripciones del cargo frente a sus funciones y los programas de capacitación son ajustados con base en dichos resultados?	1		
		Las descripciones de los cargos poseen el perfil requerido para cada cargo y las habilidades o competencias con las que se debe cumplir para el cargo (Corporativas o Especificas del cargo)?	1		
			100%	0%	
Asignación de Autoridad y Responsabilidad.	6-A. Asignación de responsabilidad y delegación de autoridad para cumplir objetivos, metas, funciones y requerimientos obligatorios (Empoderamiento).	El proceso de asignación de autoridad y responsabilidad es revisado periódicamente por la Alta Gerencia para asegurar que está funcionando adecuadamente?	1		
		Para el Director Ejecutivo (Presidente) se tiene en la descripción de su cargo definida la responsabilidad sobre el Sistema de Control Interno y la propiedad sobre dicho Sistema?	1		
		Se encuentran definidos los roles de liderazgo y dirección de los Administradores de las áreas de la Entidad (Ver Estructura Jerárquica)?	1		
		Para el Consejo de Directores (primer nivel directivo) se tiene en la descripción de los cargos definida la responsabilidad sobre el Sistema de Control Interno?	1		
		Se observa mucho personal realizando trabajos fuera del horario de trabajo?		1	
			80%	20%	

EVALUACIÓN DEL AMBIENTE DE CONTROL ENTIDAD EDUCATIVA					
COMPONENTE	AMBIENTE DE CONTROL				
FACTOR A EVALUAR	ÍTEMS QUE COMPONEN EL FACTOR A EVALUAR	DESCRIPCIÓN DE LAS PRUEBAS A REALIZAR	SI	NO	NO APLICA
Políticas y Prácticas de Recursos Humanos.	7-A. Definición e Implementación de la Cultura Organizacional.	Se posee una Cultura Organizacional definida e implementada que caracterice la entidad?	1		
		Dicha Cultura Organizacional contiene o refuerza las competencias, valores o principios corporativos, entre otros aspectos que fortalecen el ambiente de control?	1		
		Se comunica o divulga adecuadamente a todos los niveles de la organización la Cultura Organizacional?	1		
	7-B. Aplicación de procedimientos y políticas para vinculación, entrenamiento, promoción y compensación	La vinculación y contratación de personal cumple con lo establecido en la ley?	1		
		Se realiza el entrenamiento en el cargo y se deja el debido registro con la firma del funcionario como evidencia de que se realizó el entrenamiento requerido para el cargo?		1	
		Se realicen promociones o convocatorias internas para dar oportunidad a los empleados de la entidad de ocupar cargos requeridos en la estructura jerárquica para los cuales cumplan con el perfil requerido?	1		
		Se poseen claramente definidos los criterios para promociones e incrementos salariales, de tal forma que los empleados reconocen los "aspectos" premiados por la Entidad?	1		
	7-C. Adecuada evaluación experiencia de candidatos	Se evalúa la experiencia requerida de los candidatos para un cargo como parte del perfil que se debe cumplir, durante el proceso de selección de personal?	1		
	7-D. Adecuados criterios de retención y promoción	El personal de supervisión se reúne periódicamente con los supervisados para repasar los objetivos de las responsabilidades asignadas y sugerir mejoras?	1		
		Se verifica que los objetivos/ expectativas impuestas a los empleados (especialmente a los nuevos) son realistas, y están ligados con el proceso de evaluación de desempeño?	1		
		Se poseen claramente definidos los criterios de promoción y de retención de los empleados mediante beneficios a los mismos?	1		
		Se posee una adecuada transparencia y objetividad en el proceso de verificación de la satisfacción de los empleados y del clima organizacional?	1		
		Se poseen acciones de mejora tomadas a partir de los resultados de las evaluaciones de la satisfacción de los empleados y del clima laboral?	1		
	7-E. Conveniencia de las acciones remediales en respuesta a las desviaciones de las políticas y procedimientos	Se poseen implementados y formalizados procesos disciplinarios y de sanciones, que sean convenientes y dictaminen las acciones remediales que deben ser desarrolladas en respuesta a las desviaciones del cumplimiento de las políticas y procedimientos aprobados por la entidad?		1	
				86%	14%

ANEXO II: MATRIZ DE RIESGO DE TI

PUNTOS DE EVALUACION		SI	NO	N/A	Observaciones
1. PLANEACIÓN Y ORGANIZACIÓN TI		100,00%			
1.1. Plan Estratégico de TI		100,00%			
1	Se tiene definido y aprobado según acuerdo en Consejo Superior de la entidad educativa un Plan Estratégico de Tecnologías de Información que incluya objetivos de largo plazo		1		La empresa no cuenta con plan estratégico para el área de TI, toda inversión que se realiza es en base a necesidades.
2	El Plan Estratégico de Tecnologías de la Información se aplica y evalúa con regularidad de acuerdo a la política definida para su revisión y el resultado se conoce según Consejo Superior		1		No existen evaluaciones
1.2. Organización y Relaciones de TI		0,00%			
3	Dentro de la estructura organizacional de la entidad está definida la unidad administrativa Tecnología de Información (TI).	1			
4	Existencia y aplicación de metodología de desarrollo y mantenimiento de sistemas, debidamente documentada mediante papel o registro electrónico, la cual es de uso obligatorio para todas aquellas aplicaciones de la Entidad (ya sea de desarrollo interno o externo).	1			
5	Existen en la entidad funcionarios que estén en la capacidad de dar mantenimiento al sistema de información de la entidad (salidos contables, facturación entre otros) y que tengan dentro de sus funciones y responsabilidades la ejecución de esa labor.	1			
2. GESTIÓN DE TI		75,00%			
6	Se realizan diagnósticos y pruebas sobre el rendimiento y tiempo de respuesta del sistema según la política o procedimiento documentado mediante papel o registro electrónico y se implementan las recomendaciones que surgen producto de la revisión.	1			
7	Existencia y aplicación de procedimientos documentados mediante papel o registro electrónico para ejecutar pruebas de los cambios al sistema antes de ponerlos en ambiente de producción.	1			
8	La entidad educativa cuenta con un área especializada que administre la seguridad de la información		1		La administración de la seguridad esta ejecutado por la persona que tiene el rol de DBA, siendo esta persona la que ejecuta la asignación de roles en el sistema y en la base de datos.
9	El área de TI cuenta con documentación donde se detalle las funciones, responsabilidades de cada cargo	1			
3. CONTRATOS A TERCEROS		0,00%			
10	Si algún elemento de Tecnología de Información es suministrado por un tercero, existe un contrato de servicios y en este último caso se incluye una cláusula que exija la delimitación clara y asignación de funcionarios, prioridades y/o áreas para la atención inmediata de las responsabilidades afines	1			
11	Existen cláusulas contractuales que obliguen al proveedor a mantener las características de seguridad y confidencialidad de la información.	1			
12	Existencia y aplicación de cláusulas contractuales, con sus respectivas sanciones, para regular los tiempos de respuesta máximos ante fallas de computadoras, equipo de comunicaciones, software de aplicación, mantenimiento de equipo y de los sistemas automatizados.	1			
13	Existencia y aplicación de cláusulas en el contrato con sus respectivas acciones en las que se definen las responsabilidades de cada una de las partes ante situaciones contingentes o fallas graves en los servicios prestados.	1			

PUNTOS DE EVALUACION		SI	NO	N/A	Observaciones
4. SEGURIDAD FÍSICA		0,00%			
14	Se cuenta con una planta de energía eléctrica que se activa ante cortes de fluido eléctrico.	1			
15	El cableado eléctrico del equipo de cómputo se encuentra conectado a la planta de energía eléctrica y a una fuente ininterrumpida de poder (UPS).	1			
16	Existencia y aplicación de un mecanismo de acceso que restrinja y registre el ingreso de funcionarios no autorizados al área de servidores.	1			
17	En el área de servidores se cuenta con aire acondicionado, controlador de humedad y detectores de humo todo en buen funcionamiento.	1			
18	Existe dentro de la entidad, un lugar con acceso restringido y formalmente definido, donde se almacenan los respaldos y software de carácter general de entidad.	1			
19	Existe un lugar fuera de la institución donde se almacenan adecuadamente las cintas de respaldo y un registro de la entrada y salida de respaldos a ese lugar.	1			
5. SEGURIDAD LÓGICA Y DATOS		33,33%			
20	Se cuenta con un servidor o un área para desarrollo separada del servidor o área de producción.	1			
21	Existencia y aplicación de políticas y directrices documentadas, mediante papel o registro electrónico, relacionadas con el manejo y trasiego de archivos electrónicos por parte de los funcionarios, actualización de antivirus tendientes a minimizar el contagio y propagación de virus.	1			
22	Existencia y aplicación de procedimientos, documentados en papel o registro electrónico, que indiquen a los funcionarios de soporte cuáles son las acciones a seguir cuando se detecta un virus en las estaciones de trabajo o en los servidores.		1		Las actividades correctivas que se ejecutan es en base a la experiencia y criterio de la persona que las realiza, no se procede en forma estándar y no genera documentación de la misma.
6. RESPALDOS		0,00%			
23	Existencia y aplicación de un procedimiento, documentado en papel o registro electrónico, para el respaldo de la aplicación (fuentes y ejecutables) y base de datos, el cual define la periodicidad y las copias que deben mantenerse.	1			
24	La organización del proceso de respaldo permite asegurarse de que en caso de una contingencia la pérdida de información sea mínima.	1			
25	Existencia y aplicación de un procedimiento, documentado en papel o medio electrónico, de recuperación de información parcial o total ante una contingencia.	1			
26	Se realizan pruebas periódicas de recuperación para determinar que los respaldos están funcionando adecuadamente y se documentan.	1			

PUNTOS DE EVALUACION		SI	NO	N/A	Observaciones
7. BASE DE DATOS		0,00%			
27	Se tiene definido una persona o grupo de personas para la administración de la base de datos en la entidad.	1			
28	Se realizan, de acuerdo con la política o procedimiento documentado mediante papel o registro electrónico, procesos de optimización con el fin de mantener un adecuado nivel de rendimiento.	1			
29	Se tienen definidos y se aplican perfiles de acceso para los funcionarios en la base de datos aparte de los del sistema.	1			
30	Se utilizan las fortalezas de validación de información que ofrece la base de datos (triggers o integridad referencial o validaciones personalizadas por el programador).	1			
8. SOFTWARE Y HARDWARE		66,67%			
31	La entidad cuenta con un plan de renovación de equipo basado en una estrategia documentada en papel o registro electrónico, para evaluar los requerimientos de hardware de tal forma que se fundamenten en análisis técnicos para la adquisición de servidores, estaciones de trabajo y otros equipos de TI.		1		La entidad educativa no cuenta con políticas documentadas donde se establezca la evaluación de forma periódica y documente el resultado de las mismas.
32	Se cuenta con mantenimiento de las licencias del software que se utiliza en la entidad.		1		El mantenimiento de licencias lo realizan bajo demanda, a excepción de las de la base de datos.
33	Existencia y aplicación de procedimientos documentados en papel o registro electrónico o contratos, según corresponda, para el mantenimiento de los equipos de cómputo.	1			
9. RED INTERNA		66,67%			
34	Se cuenta con un administrador o grupo de personas, así establecido en la entidad, que se dedique a la administración de la red.	1			
35	Existencia y aplicación de políticas y procedimientos documentados mediante papel o registro electrónico, para proceder ante anomalías detectadas en el monitoreo de la red interna.		1		La entidad educativa no cuenta con políticas documentadas donde se establezca las acciones en caso de eventos de falla de red, por lo que en caso de que se presenten no registra información histórica de los eventos.
36	Se realizan análisis para asegurar el equilibrio entre las cargas de trabajo, tiempos de respuesta y eficiencia de la red de acuerdo con la política.		1		La entidad educativa no cuenta con políticas documentadas donde se establezca políticas para la medición de cargas y tiempos de los equipos que son parte de la infraestructura de la entidad, por lo que no registra información histórica de tiempos que se determinen como aceptables.
10. COMUNICACIONES		0,00%			
37	Se tiene definido un funcionario o grupo de funcionarios responsables del área de comunicaciones con sus funciones y responsabilidades formalmente definidas.	1			
38	La entidad cuenta con un muro de fuego en funcionamiento.	1			
39	Se tiene definida una zona desmilitarizada (DMZ) en la configuración de la red para la publicación de Internet y otros archivos de acceso público de la entidad.	1			

PUNTOS DE EVALUACION		SI	NO	N/A	Observaciones
11. CONTINUIDAD Y CONTINGENCIA		100,00%			
40	Se tiene definido y en funcionamiento un plan de contingencia y/o continuidad del negocio en la entidad.		1		La entidad educativa actualmente no cuenta con un plan de continuidad del negocio y se encuentran en un proceso de elaboración del plan de contingencia de TI.
41	Existencia y aplicación de un procedimiento documentado en papel o registro electrónico para mantener actualizado el plan de contingencia y/o continuidad del negocio.		1		No existen evaluaciones
12. INTERNET		0,00%			
42	Se le tiene definida una contraseña y usuario a los que desean realizar transacciones en la red.	1			
43	Existencia y aplicación de un procedimiento documentado en papel o registro electrónico para la solicitud de esta contraseña y usuario a los y se está aplicando.	1			Las solicitudes de usuarios y contraseñas se realiza mediante correos.
44	El área o página de consulta de los usuarios se desactiva después de cierto tiempo de no uso.	1			
45	La información que está disponible en Internet es replicada diariamente.	1			
46	La información sensible es transmitida por Internet o Intranet solo si ha sido encriptada y el destino ha sido autenticado.	1			

PUNTOS DE EVALUACION		SI	NO	N/A	Observaciones
13. USUARIOS Y CONTRASEÑAS		9,09%			
47	Existencia y aplicación de un procedimiento documentado en papel o registro electrónico, que permita solicitar la modificación, inclusión, desactivación y eliminación de perfiles en el Sistema.	1			
48	Se tienen habilitadas las facilidades de uso de contraseña que ofrece el software de red para los usuarios.	1			
49	Se utilizan sanas prácticas para el uso de contraseñas (vencimiento periódico para los password de red, restricción de uso del mismo password, cambio de password por primera vez, cambio personalizado de password)	1			
50	La estructura de la palabra de paso es tal que requiere de una combinación de caracteres que no le permite ingresar palabras de fácil pronunciación.	1			
51	La palabra de paso se almacena en forma encriptada.	1			
52	Existencia y aplicación de un procedimiento documentado en papel o registro electrónico, para la solicitud de ingreso, bloqueo o eliminación de un usuario al sistema.	1			
53	Existencia y aplicación de una política de revisión periódica de los derechos concedidos a los usuarios.		1		No existe política documentada sobre la revisión periódica de los usuarios activos y privilegios de los mismos, pero se realiza esta actividad bajo criterio del DBA y se registra en documento que no es formal para la empresa.
54	Los usuarios definidos son usados solamente por un funcionario.	1			
55	Si una sesión en el sistema se queda abierta por un periodo determinado de tiempo sin actividad, la aplicación se bloquea para que el Sistema no sea utilizado.	1			
56	El usuario de ingreso al sistema se bloquea después de un número determinado de intentos fallidos de ingreso.	1			
57	Los perfiles de acceso definidos en el Sistema identifican en forma independiente las tareas y procesos a los que tienen acceso los usuarios de acuerdo con sus funciones y responsabilidades. Y además en la aplicación se muestran solo las Opciones a las que tiene acceso el funcionario con ese perfil.	1			

PUNTOS DE EVALUACION		SI	NO	N/A	Observaciones
14. BITÁCORAS		29,17%			
14.1. Sistemas de Información		25,00%			
58	Se tienen bitácoras de los errores de validación que se generan en el procesamiento de la información y se le da seguimiento.	1			
59	Se hacen revisiones periódicas de las bitácoras de acceso al Sistema.		1		No existe política documentada sobre la revisión periódica de accesos de usuarios activos, pero se realiza esta actividad bajo criterio del DBA y se registra en documento que no es formal para la empresa.
60	Existe a nivel de la Entidad un funcionario que tiene dentro de sus funciones y responsabilidades formales la asignación de los roles o determinación los perfiles dentro del sistema.	1			
61	Cuando se efectúan cambios en los siguientes campos de información de los (cédulas, fechas de nacimiento, número de boletas de bolsa, entre otros) quedan registrados en la bitácora.	1			
14.2. Red Interna		33,00%			
62	El software de red cuenta con bitácoras activas que permita dejar pistas ante anomalías de acceso o violación de recursos en la red. (Red Interna)	1			
63	Se realizan revisiones periódicas de las bitácoras disponibles por el software de red. (Red Interna)	1			
64	Existencia y aplicación de políticas definidas que se deban tomar ante la detección de una anomalía en las bitácoras. (Red Interna)		1		No existe política documentada sobre las acciones a tomarse en caso de anomalías detectadas, por tal motivo no se cuenta con historial y acciones previas ejecutadas.
14.3. Comunicaciones		0,00%			
65	Se realizan revisiones periódicas de la bitácora que generan los diferentes dispositivos de comunicaciones (Firewall, proxy, etc.).	1			

PUNTOS DE EVALUACION		SI	NO	N/A	Observaciones
15. TI EN RIESGOS		62,22%			
15.1. Ajustes		100,00%			
66	Dispone la entidad autorizada de aplicaciones para la realización de las pruebas backtesting y stresstesting.		1		Las pruebas que se realizan no es mediante herramientas especializadas.
67	Verificar la existencia y uso de programas informáticos que permitan determinar todas aquellas operaciones que se desvíen de los parámetros aprobados		1		No existe
15.2. Suministro de Información		0,00%			
68	Se generan automáticamente a partir de las bases de datos de la entidad educativa los archivos con la información que debe ser remitida al organo supervisor	1			
69	Dispone la entidad de los principales módulos TI debidamente integrados de tal forma que esa integración está diseñada de tal forma que los cálculos y resultados de distintas variables que se ejecutan en determinado módulo son utilizados por los otros, cuando así se requiere, sin necesidad de realizar otros cálculos de la misma variable.	1			
70	Permite el sistema la generación de información histórica de saldos contables de todas las cuentas en cualquier momento en el tiempo	1			

PUNTOS DE EVALUACION		SI	NO	N/A	Observaciones
15.3. Integridad de los sistemas y herramientas de auditoría		55,00%			
71	La Entidad cuenta con auditorías internas o externas		1		Las auditorías formales que se han realizado son una, otras efectuadas son con efectos didácticos, es decir como proyectos. La entidad no cuenta con auditoría interna.
72	La Entidad da seguimiento a las recomendaciones de la Auditoría Interna o Externa en relación con la evaluación de los sistemas.	1			El resultado de la única auditoría externa fue trabajar en la elaboración de un DRP, lo cual la entidad se encuentra en proceso de implementación.
73	Existe documentación técnica para cada uno de los procesos que ejecuta el sistema y que concuerda con lo programado.		1		La entidad no cuenta con documentación de los sistemas ni a nivel funcional ni técnico, por lo que el riesgo de ejecutar las actividades de forma no periódica existe para el caso funcional, para el caso técnico la curva de aprendizaje es más alta.
74	Existen manuales de usuario y del sistema definidos para cada uno de los módulos que componen el sistema de información, su integración y mantenimiento continuo.		1		La entidad no cuenta con documentación de los sistemas ni a nivel funcional ni técnico, por lo que el riesgo de ejecutar las actividades de forma no periódica existe para el caso funcional, para el caso técnico la curva de aprendizaje es más alta.
75	Se tiene control de los tipos de datos sobre los campos que se capturan.	1			
76	Se permite ingresar transacciones con el mismo número de identificación o llave (repetidos)		1		
77	El sistema lleva un consecutivo propio de las diferentes transacciones que permite realizar la aplicación y se controla el orden cronológico de ingreso de transacciones en el sistema, de tal forma que no permita realizar operaciones en forma extemporánea o de periodos anteriores.	1			
78	Existe a nivel de la Entidad una política definida para que el sistema de información cuente con validaciones propias que se van ejecutando conforme se realizan las operaciones diarias de la entidad.	1			
79	Si el sistema emite archivos electrónicos como salida, se graban en un área con acceso restringido.		1		Los archivos que se generan por el proceso de facturación se depositan en la máquina del usuario que los genera.
80	Los reportes cuentan con nombre, fecha de emisión, usuario que lo emitió y programa que los elaboró en ellos cada vez que son impresos.	1			
81	Se tiene alguna disposición establecida en términos de manipulación, archivado o destrucción de los reportes que emite el sistema.	1			