



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
ESCUELA DE INGENIERÍA EN CONTABILIDAD Y AUDITORÍA

TESIS DE GRADO

Previo a la obtención del Título de:
Ingeniero en Contabilidad y Auditoría CPA.

TEMA:

Auditoría Informática al Instituto Ecuatoriano de Crédito Educativo y Becas (IECE)
Regional 3 Riobamba, período 2012.

Autor:

Alex Mauricio Obando Yumisaca

Riobamba - Ecuador

2014

CERTIFICACIÓN DEL TRIBUNAL

Certificamos que el presente trabajo ha sido revisado en su totalidad, quedando autorizada su presentación.

Ing. Byron Napoleón Cadena Oleas

DIRECTOR DE TESIS

Ing. Mayra Alejandra Oñate Andino

MIEMBRO DEL TRIBUNAL

CERTIFICACIÓN DE AUTORÍA

Las ideas expuestas en el presente trabajo de investigación y que aparecen como propias, son en su totalidad de absoluta responsabilidad del autor.

Alex Mauricio Obando Yumisaca

DEDICATORIA

A Dios, por haberme dado la vida, ser mi guía, darme fuerzas para salir adelante y afrontar con valentía las adversidades sin perder nunca la dignidad ni desfallecer en el intento.

A mis padres Víctor Obando y Cecilia Yumisaca, quienes me han dado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi empeño, mi perseverancia, mi coraje para conseguir mis objetivos.

A mi hermana y a toda mi familia por sus palabras de aliento y estar presente en cada etapa de mi vida.

ALEX OBANDO

AGRADECIMIENTO

Le agradezco a Dios por haberme acompañado y guiado a lo largo de toda mi carrera.

A mí querida familia por su comprensión y apoyo incondicional en todo momento.

A los catedráticos de mi querida Escuela Ingeniería en Contabilidad y Auditoría quienes han sido un pilar fundamental para mi formación.

Al Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba, por permitirme desarrollar el proyecto de tesis en la entidad, a la unidad de TICs por todo su apoyo y colaboración para el desarrollo y culminación del mismo.

A los Ingenieros Napoleón Cadena y Alejandra Oñate quienes con su paciencia y conocimiento supieron aportar para la elaboración y culminación de la presente tesis.

Índice Contenido

PORTADA.....	I
CERTIFICACIÓN DEL TRIBUNAL	II
CERTIFICACIÓN DE AUTORÍA.....	III
DEDICATORIA	4
AGRADECIMIENTO	5
ÍNDICE DE FIGURAS.....	9
ÍNDICE DE TABLAS	9
INTRODUCCIÓN	10
CAPÍTULO I	
1.GENERALIDADES DEL INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS (IECE) REGIONAL 3 RIOBAMBA	11
1.1. IDENTIFICACIÓN DE LA INSTITUCIÓN	11
1.2. UBICACIÓN GEOGRÁFICA.....	11
1.3. RESEÑA HISTÓRICA.....	12
1.4. BASE LEGAL	14
1.5. OBJETIVOS ESTRATÉGICOS DEL IECE	16
1.6. OBJETIVOS ESPECÍFICOS DEL IECE	16
1.7. ORGANIGRAMA ESTRUCTURAL DEL INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS (IECE) REGIONAL 3 RIOBAMBA	17
1.8. MISIÓN INSTITUCIONAL.....	18
1.9. VISIÓN INSTITUCIONAL	18
1.10. AUTORIDADES INSTITUCIONALES	18
CAPÍTULO II	
2. LA AUDITORÍA	19
2.1. AUDITAR.....	19
2.2. ANTECEDENTES.....	19
2.3. DEFINICIÓN DE AUDITORÍA	20
2.4. IMPORTANCIA DE LA AUDITORÍA	21
2.5. CARACTERÍSTICAS DE LA AUDITORÍA	21
2.6. CLASIFICACIÓN DE LA AUDITORÍA	22
2.6.1.DE ACUERDO A QUIENES REALIZAN EL EXAMEN.....	24
2.6.2. AUDITORÍAS POR SU ÁREA DE APLICACIÓN	23
2.7. AUDITORÍA INFORMÁTICA.....	25
2.7.1. ANTECEDENTES DE LA AUDITORÍA INFORMÁTICA	25

2.7.2. ALCANCE.....	26
2.7.3. DEFINICIÓN DE AUDITORÍA INFORMÁTICA.....	26
2.7.4. IMPORTANCIA DE LA AUDITORÍA INFORMÁTICA	27
2.7.5. OBJETIVOS DE LA AUDITORÍA INFORMÁTICA	28
2.7.6. TIPOS DE AUDITORÍA INFORMÁTICA	28
2.8. CONTROL INTERNO INFORMÁTICO.....	32
2.8.1. OBJETIVOS DEL CONTROL INTERNO INFORMÁTICO.....	32
2.8.2. TIPOS DE CONTROLES INTERNOS	33
2.9. PROCESO DE AUDITORÍA INFORMÁTICA	34
2.10. INSTRUMENTOS DE RECOPIACIÓN EN LA AUDITORÍA INFORMÁTICA	36
2.11. PAPELES DE TRABAJO	38
2.12. PROGRAMAS DE AUDITORÍA	39
2.13. HALLAZGOS DE AUDITORÍA.....	41
2.14. MARCAS DE AUDITORÍA	42
2.15. COMUNICACIÓN DE RESULTADOS DE AUDITORÍA	42
2.16. NORMAS DE CONTROL INTERNO PARA LA AUDITORÍA INFORMÁTICA	43
CAPÍTULO III	
3. DIAGNÓSTICO SITUACIONAL DEL INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS (IECE) REGIONAL 3 RIOBAMBA	46
3.1. DIAGNÓSTICO SITUACIONAL.....	46
3.2. ANÁLISIS FODA.....	46
3.2.1. MATRIZ FODA	46
3.2.2. ANÁLISIS DE MEDIOS INTERNOS	47
3.2.3. ANÁLISIS DE MEDIOS EXTERNOS	55
CAPÍTULO IV	
4. AUDITORÍA INFORMÁTICA AL INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS (IECE) REGIONAL 3 RIOBAMBA	61
4.1 GENERALIDADES	61
4.1.1 ALCANCE.....	61
4.1.2 OBJETIVO	61
4.1.3 BASE LEGAL	61
4.1.4 METODOLOGÍA.....	61
4.1.5 HOJA DE MARCAS	69
4.1.6 ABREVIATURAS.....	70
ETAPAS DE LA AUDITORÍA INFORMÁTICA.....	71
PRIMERA ETAPA: PLANEACIÓN	71
SEGUNDA ETAPA: EJECUCIÓN.....	81

TERCERA ETAPA: DETERMINACIÓN DE HALLAZGOS	94
CUARTA ETAPA: COMUNICACIÓN DE RESULTADOS	102
CAPÍTULO V	
5. CONCLUSIONES Y RECOMENDACIONES.....	113
5.1 CONCLUSIONES	113
5.2 RECOMENDACIONES	115
RESUMEN	116
ABSTRACT.....	¡Error! Marcador no definido.
BIBLIOGRAFÍA	118
LINKOGRAFÍA	119
ANEXOS	194

ÍNDICE DE FIGURAS

Figura 1: Logotipo Institucional.....	11
Figura 2: Plano de Ubicación.....	12
Figura 3: Organigrama institucional	17
Figura 4: Organigrama Institucional	75
Figura 5: Organigrama Institucional	107

ÍNDICE DE TABLAS

Tabla 1: Información Geográfica	11
Tabla 2: Autoridades Institucionales.....	18
Tabla 3: Proceso de Auditoría Informática	34
Tabla 4: Instrumentos de Recopilación en la Auditoría Informática	36
Tabla 5: Estructura del Programa de Auditoría.....	40
Tabla 6: Marcas de Auditoría.....	42
Tabla 7 Normas de Tecnología de la información	44
Tabla 8: Matriz FODA	46
Tabla 9: Análisis de medios internos	48
Tabla 10: Perfil Estratégico Interno	51
Tabla 11: Ponderación Perfil Estratégico Interno	53
Tabla 12: Análisis de Medio Externo.....	55
Tabla 13: Perfil Estratégico Externo	58
Tabla 14: Ponderación Perfil Estratégico Externo	59

INTRODUCCIÓN

La presente Tesis denominada “Auditoría Informática al Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba, período 2012”; ha sido realizada debido a la necesidad que presenta la institución en conocer, verificar y evaluar el cumplimiento de procedimientos en el manejo y control de los recursos informáticos existentes en la entidad; para ello, la ejecución está basada en cinco capítulos descritos a continuación:

El primer capítulo trata sobre las generalidades de la institución: identificación, reseña histórica, base legal, objetivos institucionales, estructura organizacional, misión, visión, y autoridades.

El segundo capítulo describe el marco conceptual que comprende los fundamentos de auditoría y auditoría informática; siendo una base para la ejecución del trabajo en estudio.

El tercer capítulo puntualiza un diagnóstico FODA, mediante un análisis interno y externo con el fin de determinar sus fortalezas y debilidades en factores relacionados con el área informática, y al mismo tiempo identificar las oportunidades y amenazas que se presenten en el entorno de la institución.

El cuarto capítulo, trata el desarrollo de la Auditoría Informática en base a las fases como son: planeación de la auditoría, ejecución de la auditoría y la presentación del informe de auditoría.

El quinto capítulo, el último, señala las conclusiones y recomendaciones respectivas.

Para el desarrollo del presente tema de Auditoría Informática se tomó como base las Normas de Control Interno de la Contraloría General del Estado (CGE), en lo referente a Tecnologías de Información y Comunicación que permitieran evaluar la utilización y aprovechamiento de los recursos informáticos, además de emitir nuestro criterio respaldado con los papeles de trabajo obtenidos en el transcurso de la investigación.

CAPÍTULO I

1. GENERALIDADES DEL INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS (IECE) REGIONAL 3 RIOBAMBA

1.1. IDENTIFICACIÓN DE LA INSTITUCIÓN

➤ **Nombre de la Institución:**

Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba.

Figura 1: Logotipo Institucional



- **Tipo de institución:** Servicios.
- **País:** Ecuador.
- **Provincia:** Chimborazo.
- **Ciudad:** Riobamba.
- **Parroquia:** Veloz.
- **Dirección:** 10 de Agosto N° 2172 y Espejo (esquina, edificio del Correo).
- **Teléfono:** Tel. 03 2942336 / 2942335 / 2961514
- **Email:** riobamba@iece.fin.ec¹

1.2. UBICACIÓN GEOGRÁFICA

Tabla 1: Información Geográfica

Ubicación	Parte central de callejón interandino del Ecuador
Provincia	Chimborazo
Ciudad	Riobamba
Temperatura	Mínima 10° C Máxima 18° C
Superficie delimitada por el perímetro urbano	1150,2 km ²

¹ Información adquirida IECE

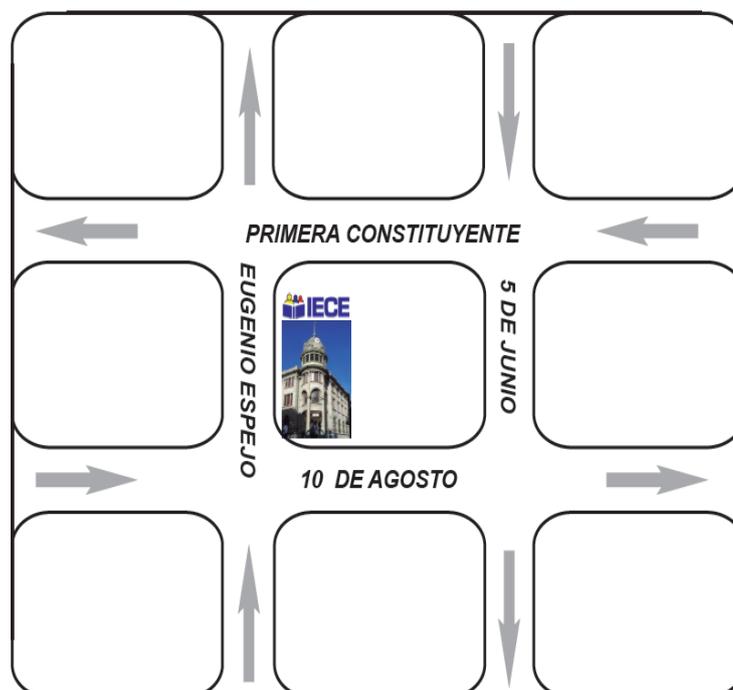
Huso Horario	-5:00 GMT.
Parroquias urbanas	Maldonado, Veloz, Lizarzaburu, Velasco y Yaruquíes
Parroquias rurales	Cacha, Calpi, Cubijíes, Flores, Licán, Licto, Pungalá, Punín, Químiag, San Juan, San Luis

Fuente: Instituto Ecuatoriano de Crédito Educativo y becas IECE Regional 3 Riobamba

Elaborado por: Autor de Tesis

➤ **Plano de ubicación:**

Figura 2: Plano de Ubicación



Fuente: Instituto Ecuatoriano de Crédito Educativo y Becas IECE Regional 3 Riobamba

Elaborado por: Autor de la Tesis

1.3. RESEÑA HISTÓRICA

El Instituto Ecuatoriano de Crédito Educativo y Becas (IECE), es una entidad pública creada el 26 de abril de 1971 por el Presidente de la República Dr. José María Velasco Ibarra, quien firma el Decreto No. 601, publicado en Registro Oficial 212 del mismo año, con la finalidad de que administre y coordine los recursos destinados a apoyar a los estudiantes.

En el gobierno presidido por el General Guillermo Rodríguez Lara, se expide el decreto supremo N° 1272 del 7 de noviembre de 1972, publicado en el registro oficial 182 de 13 de los mismos mes y año, por el cual se reforma el decreto 601 que había creado el Instituto

Ecuatoriano de Crédito Educativo, IECE, dotándole de una nueva estructura y de mayor financiamiento para que pueda cumplir debidamente los propósitos para los que fue creado.

La entidad empezó a funcionar en marzo de 1973, teniendo como su primer director ejecutivo, al Dr. Ricardo Muñoz Chávez, quien asumió el reto de organizar la institución administrativa y financieramente, las primeras oficinas del IECE se instalaron en el edificio alambra, situado entre las calles Salinas y Santiago de la ciudad de Quito.

En la ciudad de Riobamba el Instituto Ecuatoriano de Crédito Educativo y Becas IECE empezó a laborar en el año 1976 a cargo del Delegado Lic. Luis Pazmiño.

Para cumplir con la misión de financiar la formación académica a las ecuatorianas y ecuatorianos, se firman los siguientes decretos que aseguran su financiamiento:

APORTE MINERO: Mediante Decreto Supremo No. 101 publicado en Registro Oficial 484 de 31 de diciembre de 1974, en su Art. 96 se establece la obligación de los contratistas o asociados, de pagar 10 centavos de sucre por cada tonelada de mineral extraído.

APORTE PETROLERO: Mediante Decreto Supremo No. 982 de 21 de noviembre de 1975, se sustituyó el gravamen de 20 centavos de sucre por cada barril de petróleo producido, que fuera destinado al IECE en el Decreto de su creación.

APORTE PATRONAL: A mediados de los años 70 la creciente demanda de crédito educativo y la disminución de los recursos asignados al IECE, ocasionaron una grave crisis financiera a la institución, que obligó al IECE a suspender la concesión de nuevos créditos y dedicarse exclusivamente a atender los desembolsos por los contratos suscritos con anterioridad. Es así que el 3 de agosto de 1976 se le otorga la transferencia del 0,5% de las planillas de pago al Instituto Ecuatoriano de Seguridad Social que realizan las empresas públicas y privadas, según decreto Supremo 623-A.

ADMINISTRACIÓN DE BECAS INTERNACIONALES: Mediante Decreto Supremo No. 247 de 5 de marzo de 1974, publicado en el Registro Oficial 510 de 12 de los mismos mes y año, el General Guillermo Rodríguez Lara transfiere al IECE la administración de las becas internacionales de estudios, entrenamiento y perfeccionamiento en el exterior, inclusive las referentes a las de Cooperación Técnica Internacional.

REGLAMENTOS DE SELECCIÓN DE BECARIOS: El 19 de agosto de 1981 el Consejo Directivo del IECE dicta una resolución que contiene el reglamento para la aplicación del Art. 6 de la Ley Constitutiva Codificada del IECE, y regula el funcionamiento de la Comisión Mixta de Selección de Becarios en base a un proyecto aprobado por el Comité de Cooperación Técnica y Asistencia Económica, al que pertenece dicha Comisión Mixta. La Asesoría Jurídica de la Presidencia de la República, mediante oficio No. 82-137-DAJ-SGA de 5 de abril de 1982, emite opinión favorable para la expedición de este reglamento por parte del Consejo Directivo del Instituto.

En la administración de la Lcda. Alba Luz Mora, en el afán de contar con un cuerpo legal que esté acorde con los nuevos retos del derecho financiero y con las operaciones que realiza la institución, mediante registro oficial No.179 del 03 de enero del 2006, se expide la ley sustitutiva a la ley del IECE, la misma que busca, entre otras cosas, "coordinar a través de un solo organismo la responsabilidad de la administración de los recursos financieros, así como las becas nacionales e internacionales". Este nuevo cuerpo legal fortaleció y consolidó a la institución en todos sus ámbitos, otorgándole su propia legislación operativa, administrativa y financiera.

Es a partir de junio del 2007, y con el nombramiento del doctor Fabián Solano Moreno, como gerente general, el IECE entra en una profunda transformación de servicios y cobertura. El fortalecimiento de su infraestructura física se inicia con la adquisición de un nuevo edificio matriz, que permite brindar una mejor atención a los usuarios. La representación institucional en nuevas provincias ecuatorianas, constituye otro de los logros de la presente administración.

Durante el año 2008, se crearon nueve oficinas ubicadas en las provincias de: Orellana, Napo, Pastaza, Morona Santiago, Santo Domingo de los Tsáchilas, Bolívar, Tungurahua, El Oro, y Los Ríos. Paralelo a ello, fue necesario el mejoramiento de la infraestructura informática, fundamental para el buen desempeño de sus funcionarios (Instituto Ecuatoriano de Crédito Educativo y Beca, 2013).

1.4. BASE LEGAL

El Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba es una institución que renueva cada día su responsabilidad social de apoyar el afán de superación de la población estudiantil ecuatoriana, pues mediante el crédito educativo y las becas, se logra el sendero de un Ecuador próspero y diferente.

El IECE para el desarrollo de sus actividades cuenta con las siguientes disposiciones legales, reglamentarias y demás disposiciones internas:

Crédito

- Reglamento de Crédito Educativo.
- Manual de Gestión de Crédito.
- Manual de Procedimiento Coactivo.
- Reglamento para el Ejercicio de la Jurisdicción Coactiva.
- Reforma al Reglamento de la Jurisdicción Coactiva.

Becas

- Reglamento Becas Hijos Combatientes del CENEPA
- Instructivo para la Ejecución de Becas ECORAE
- Reforma al Instructivo para la Ejecución del Subprograma Monseñor Leónidas Proaño componente Cuba.
- Instructivo del Subprograma Eloy Alfaro componente Zamorano.
- Ley de Creación de la Beca Estudiantil de Entrenamiento.
- Reglamento Ejecución de Becas Universidad Sin Fronteras Perú-Ecuador.
- Reglamento Funcionamiento Comisión Mixta de Selección de Becarios.

Generales

- Constitución Política del Estado.
- Reglamento de Atribuciones y Deberes del Directorio.
- Reglamento de Contrataciones.
- Reglamento del Comité de Auditoria.
- Reglamento para la Selección y Eliminación de Documentos.
- Reglamento para el Pago de Dietas.
- Manual de Prevención de Lavado de Activos.
- Reglamento de Administración de RRHH.
- Reglamento para el Funcionamiento del Comité de Cumplimiento.
- Reforma al Reglamento para el Funcionamiento del Comité de Cumplimiento del IECE.
- Reglamento para la Contratación de Seguros del IECE. (IECE, La institución Leyes y Reglamentos, 2013)

1.5. OBJETIVOS ESTRATÉGICOS DEL IECE

1. Conceder crédito educativo y becas de acuerdo a los criterios de priorización establecidos en la política pública.
2. Fortalecer la estructura económica-financiera de la entidad.
3. Mejorar continuamente la administración del IECE bajo los principios constitucionales de eficacia, eficiencia, calidez a través de estándares de calidad en los servicios e infraestructura que ofrece la Institución.

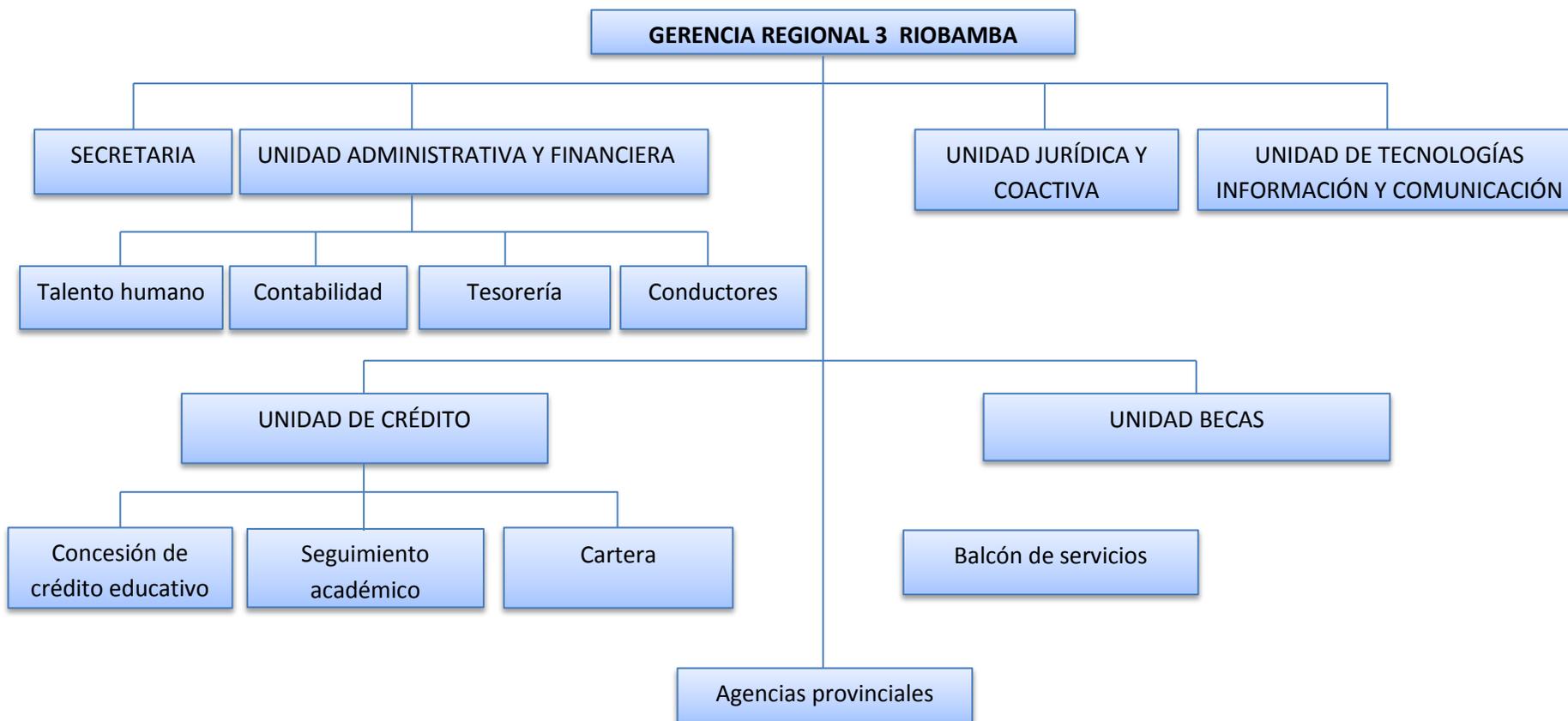
1.6. OBJETIVOS ESPECÍFICOS DEL IECE

1. Mantener y ampliar la cobertura de los servicios a nivel nacional.
2. Ejecutar la política pública para la operativización de la entrega los servicios y productos institucionales.
3. Administrar de manera eficiente los fondos y ofertas de becas provenientes de organismos e instituciones nacionales e internacionales.
4. Contar con una estructura orgánica y normativa actualizada.
5. Implementar el plan de capacitación, formación y especialización adecuada a las necesidades institucionales, conforme la normativa legal vigente.
6. Generar mecanismos de comunicación intra e inter institucional que permitan el posicionamiento de los programas del sistema de fortalecimiento al talento humano.
7. Establecer alianzas estratégicas que permitan el fortalecimiento institucional.
8. Contar con sistemas integrados acorde a la nueva tecnología, proveer a la institución el parque informático suficiente.
9. Contar con estándares de calidad a nivel nacional de los servicios e infraestructura de la Institución.
10. Bajar la mora académica (reportes académicos), con la actualización permanente
11. Mejorar la administración de cartera para disminuir la morosidad nacional a un dígito.
12. Implementar el sistema automatizado de la gestión administrativa, financiera y becas a nivel nacional, para efectuar un óptimo y adecuado control de los recursos institucionales.
13. Desarrollar y ejecutar un plan anual de contrataciones enmarcado en los objetivos del PNBV y los objetivos Institucionales.
14. Coadyuvar a que las operaciones de crédito se realicen con el mínimo de riesgo.
(IECE, La institución Misión. Visión, 2013)

1.7. ORGANIGRAMA ESTRUCTURAL DEL INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS (IECE) REGIONAL 3 RIOBAMBA

Para el cumplimiento de su misión, visión y objetivos, el Instituto Ecuatoriano de Crédito Educativo y Becas – Regional 3 Riobamba cuenta con la siguiente Estructura Orgánica:

Figura 3: Organigrama institucional



Fuente: Reglamento Orgánico de Gestión por Procesos del Instituto Ecuatoriano de Crédito Educativo y Becas

Elaborado por Autor de Tesis

1.8. MISIÓN INSTITUCIONAL

El IECE contribuye al desarrollo del talento humano, mediante el manejo de productos y servicios orientados a potencializar, con calidad, calidez y oportunidad las capacidades de sus beneficiarios, demostrando eficiencia en el manejo, operatividad, seguimiento y monitoreo de los programas generados a nivel nacional.

1.9. VISIÓN INSTITUCIONAL

El IECE, será el gestor de la formación y especialización del talento humano a través de la colocación de productos y servicios financieros y no financieros como el crédito educativo y las becas.

1.10. AUTORIDADES INSTITUCIONALES

Tabla 2: Autoridades Institucionales

NOMBRE	CARGO
Abg. Lenin Tito Ruilova	Gerente Regional
Lic. Martha Asqui Armas	Experta en Contabilidad Bancaria
Lic. Mariana de Jesús Goyes Armas	Experta en Tesorería Bancaria
Ing. Diana Isabel Erazo Riera	Auxiliar Contable
Ing. Marcelo Monar	Experto en Sistemas Informáticos
Dra. Susana Vaca	Experta en Cartera Bancaria
Sr. Ernesto Navela	Experto en Seguimiento Académico
Abg. Richard Villavicencio	Experto en Becas
Dr. Mario Muñoz	Experto en Asesoramiento Jurídico

Fuente: Instituto Ecuatoriano de Crédito Educativo y becas IECE Regional 3 Riobamba

Elaborado por: Autor de Tesis

CAPÍTULO II

2. LA AUDITORÍA

2.1. AUDITAR

Auditar es el proceso de acumular y evaluar evidencia, realizado por una persona independiente y competente acerca de la información cuantitativa de una entidad económica específica, con el propósito de determinar e informar sobre el grado de correspondencia existente entre la información cuantificable y los criterios establecidos. (De la Peña G., 2008)

2.2. ANTECEDENTES

La auditoría es una de las aplicaciones de los principios científicos de la contabilidad, basada en la verificación de los registros patrimoniales, para observar su exactitud; no obstante, este no es su único objetivo.

Su importancia es reconocida desde los tiempos más remotos, teniéndose conocimientos de su existencia ya en las lejanas épocas de la civilización sumeria.

Acreditase, todavía, que el termino auditor evidenciando el título del que practica esta técnica, apareció a finales del siglo XVIII, en Inglaterra.

En diversos países de Europa, durante la edad media, muchas eran las asociaciones profesionales, que se encargaban de ejecutar funciones de auditorías, destacándose entre ellas los consejos Londinenses (Inglaterra), en 1310, el Colegio de Contadores, de Venecia (Italia), 1581.

La revolución industrial llevada a cabo en la segunda mitad del siglo XVIII, imprimió nuevas direcciones a las técnicas contables, especialmente a la auditoría, pasando a atender las necesidades creadas por la aparición de las grandes empresas (donde la naturaleza en el servicio es prácticamente obligatoria).

Se preanunció en 1845, poco después de penetrar la contabilidad de los dominios científicos y ya el "Railway Companies Consolidation Act" obligaba la verificación anual de los balances que debían hacer los auditores.

También en los Estados Unidos de Norteamérica, una importante asociación cuida las normas de auditoría, la cual publicó diversos reglamentos, de los cuales el primero que conocemos data de octubre de 1939, en tanto otros consolidaron las diversas normas en diciembre de 1939, marzo de 1941, junio de 1942 y diciembre de 1943. (Esparza, 2010)

2.3. DEFINICIÓN DE AUDITORÍA

Es el examen profesional, objetivo e independiente, de las operaciones financieras y/o administrativas, que se realiza con posterioridad a su ejecución en las entidades públicas o privadas y cuyo producto final es un informe conteniendo opinión sobre la información financiera y/o administrativa auditada, así como conclusiones y recomendaciones tendientes a mejorar. (Slosse, C.A., Gordiez, J.C., Giordano Silva, 1999)

Del concepto se aprecian los siguientes elementos principales:

- Es un examen profesional, objetivo e independiente.
- De las operaciones financieras y/o Administrativas.
- Se realiza con posterioridad a su ejecución.
- Producto final es un informe.
- Conclusiones y recomendaciones.

Este examen o auditoría comprende:

1. Determinar el grado de cumplimiento de objetivos y metas de los planes administrativos y financieros.
2. Forma de adquisición, protección y empleo de los recursos materiales y humanos.
3. Racionalidad, economía, eficiencia y eficacia en el cumplimiento de los planes financieros y administrativos.

El Comité para Conceptos Básicos de Auditoría define auditoría de la siguiente manera:

"Un proceso sistemático que consiste en obtener y evaluar objetivamente evidencia sobre las afirmaciones relativas a los actos y eventos de carácter económico; con el fin de determinar el grado de correspondencia entre esas afirmaciones y los criterios establecidos, para luego comunicar los resultados a las personas interesadas".

Esta definición es un poco restringida, por cuanto reduce la auditoría a eventos solamente de carácter económico, siendo la labor de la auditoría mucho más amplia, abarcando

también aspectos administrativos, como el manejo de los recursos humanos, recursos técnicos y otros.

Tomando en cuenta los criterios anteriores se puede decir que la auditoría abarca varios aspectos entre ellos también se encuentra el área informática, lo cual se debe evaluar para que la empresa tenga un adecuado funcionamiento; por tal razón la auditoría es un examen sistemático que consiste en la emisión de una opinión profesional sobre sí el objeto sometido a análisis, cumple satisfactoriamente con las actividades establecidas por la institución.

2.4. IMPORTANCIA DE LA AUDITORÍA

Las auditorías en los negocios son muy importantes, por cuanto la gerencia sin la práctica de una auditoría no tiene plena seguridad de que los datos económicos registrados realmente son verdaderos y confiables. Es la auditoría que define con bastante razonabilidad, la situación real de la empresa.

Es común que las instituciones financieras, cuando les solicitan préstamos, pidan a la empresa solicitante, los estados financieros auditados, es decir, que vayan avalados con la firma de un CPA.

Una auditoría puede evaluar, por ejemplo, los estados financieros en su conjunto o una parte de ellos, el correcto uso de los recursos humanos, el uso de los materiales y equipos y su distribución, etc. Contribuyendo con la gerencia para una adecuada toma de decisiones. (Madariaga Gorocica, 2004)

2.5. CARACTERÍSTICAS DE LA AUDITORÍA

La auditoría en términos generales se caracteriza por:

- 1. Es objetiva:** Significa que el examen es imparcial, sin presiones ni halagos, con una actitud mental independiente, sin influencias personales ni políticas. En todo momento debe prevalecer el juicio del auditor, que estará sustentado por su capacidad profesional y conocimiento pleno de los hechos que refleja en su informe.
- 2. Sistemática:** Es sistemática porque su realización tiene una planificación adecuada y está sometida a las normas profesionales y al código de ética profesional.
- 3. Profesional:** Debido a que es ejecutada por auditores o contadores públicos a nivel universitario o equivalentes, o equipos multidisciplinarios según la modalidad o tipo de auditoría y examen especial, que poseen capacidad, experiencia y conocimientos en el

área de auditoría, quienes deben emitir un informe profesional dependiendo del tipo de auditoría de la que se trate.

4. **Selectiva:** Su ejecución se basa en pruebas selectivas, técnicamente sustentadas.
5. **Imparcial:** Es ejecutada por auditores que actúan con criterio imparcial y no tienen conflicto de intereses respecto de las actividades y personas objeto y sujeto de examen.
6. **Integral:** Porque cubre la revisión de las actividades operativas, administrativas, financieras, ecológicas e informáticas, incluye los resultados de la evaluación del control interno, la legalidad de los actos administrativos, actos normativos y actos contractuales.
7. **Recurrente:** Porque el ejercicio de la auditoría se ejecuta en forma periódica. (Monografias.com, Características de la Auditoría, 2009)

2.6. CLASIFICACIÓN DE LA AUDITORÍA

Para un mejor estudio, la auditoría se la ha clasificado de la siguiente manera:

2.6.1. DE ACUERDO A QUIENES REALIZAN EL EXAMEN.

Se refiere a la forma en que se realiza este tipo de trabajo y también como se establece la relación laboral en las empresas, donde se llevara cabo la auditoría.

- **Auditoría externa:** Aplicando el concepto general, se puede decir que la auditoría externa es el examen crítico, sistemático y detallado de un sistema de información de una unidad económica, realizado por un contador público sin vínculos laborales con la misma, utilizando técnicas determinadas y con el objeto de emitir una opinión independiente sobre la forma como opera el sistema, el control interno del mismo y formular sugerencias para su mejoramiento.

El dictamen u opinión independiente tiene trascendencia a los terceros, pues da plena validez a la información generada por el sistema ya que se produce bajo la figura de la fe pública, que obliga a los mismos a tener plena credibilidad en la información examinada.

- **Auditoría interna:** la auditoría interna es el examen crítico, sistemático y detallado de un sistema de información de una unidad económica, realizado por un profesional con vínculos laborales con la misma, utilizando técnicas determinadas y con el objeto de emitir informes y formular sugerencias para el mejoramiento de la misma. Estos informes son de circulación interna y no tienen trascendencia a los terceros pues no se producen bajo la figura de la fe pública.

Las auditorías internas son hechas por personal de la empresa. Un auditor interno tiene a su cargo la evaluación permanente del control de las transacciones y operaciones y se preocupa en sugerir el mejoramiento de los métodos y procedimientos de control interno que redunden en una operación más eficiente y eficaz. Cuando la auditoría está dirigida por contadores públicos profesionales independientes, la opinión de un experto desinteresado e imparcial constituye una ventaja definida para la empresa y una garantía de protección para los intereses de los accionistas, los acreedores y el público.

La imparcialidad e independencia absolutas no son posibles en el caso del auditor interno, puesto que no puede divorciarse completamente de la influencia de la alta administración, y aunque mantenga una actitud independiente como debe ser, esta puede ser cuestionada ante los ojos de los terceros. Por esto se puede afirmar que el Auditor no solamente debe ser independiente, sino parecerlo para así obtener la confianza del público.

- **Auditoría gubernamental:** Es gubernamental, cuando la practican auditores de la Contraloría General de la República, o auditores internos del sector público o firmas privadas que realizan auditorías en el Estado con el permiso de la Contraloría. (Madariaga Gorocica, 2004)

2.6.2. AUDITORÍAS POR SU ÁREA DE APLICACIÓN

Se refiere al ámbito específico donde se llevan a cabo las actividades y operaciones que serán auditadas, ubicando a cada tipo de auditoría de acuerdo con el área de trabajo e influencia de la rama o especialidad que será evaluada; entre estas tenemos las siguientes:

- **Auditoría Financiera:** Es la revisión sistemática, explorativa y crítica que realiza un profesional de contabilidad a los libros y documentos contables, a los controles y registros de las operaciones financieras y a la emisión de los estados financieros de una empresa, con el fin de evaluar y opinar sobre la razonabilidad, veracidad, confiabilidad y oportunidad en la emisión de los resultados financieros obtenidos durante el periodo específico o un ejercicio fiscal. El propósito final es emitir un dictamen contable sobre la correcta presentación de los resultados financieros a los accionistas, clientes, autoridades fiscales y terceros interesados, en relación a las utilidades, pago de impuestos y situación financiera y económica de la institución.
- **Auditoría administrativa:** Es la revisión sistemática y exhaustiva que se realiza a la actividad administrativa de una empresa, en cuanto a su organización, las relaciones entre sus integrantes y el cumplimiento de las funciones y actividades que regulan sus operaciones. Su propósito es evaluar tanto el desempeño administrativo de las áreas de la

empresa, como la planeación y control de los procedimientos de operación, y los métodos y técnicas de trabajo establecidos en la institución, incluyendo la observancia de las normas, políticas y reglamentos que regulen el uso de todos sus recursos.

- **Auditoría operacional:** Es la revisión exhaustiva, sistemática y específica que se realiza a las actividades de una empresa, con el fin de evaluar su existencia, suficiencia, eficacia, eficiencia y el correcto desarrollo de sus operaciones, cualesquiera que estas sean, tanto en el establecimiento y cumplimiento de los métodos, técnicas y procedimientos de trabajo necesarios para el desarrollo de sus operaciones, en coordinación con los recursos disponibles, como en las normas, políticas, lineamientos y capacitación que regulan el buen funcionamiento de la empresa.
- **Auditoría integral:** Es la revisión exhaustiva, sistemática y global que realiza un equipo multidisciplinario de profesionales a todas las actividades y operaciones de una empresa, con el propósito de evaluar, de manera integral, el correcto desarrollo de las funciones en todas sus áreas administrativas, cualesquiera que estas sean, así como de evaluar sus resultados conjuntos y relaciones de trabajo, comunicaciones y procedimientos interrelacionados que regulan la realización de las actividades compartidas para alcanzar el objeto institucional; dicha revisión se lleva a cabo también a las normas, políticas y lineamientos sobre el uso de todos los recursos de la empresa.
- **Auditoría gubernamental:** es la revisión exhaustiva, sistemática y concreta que se realiza a todas las actividades y operaciones de una entidad gubernamental, cualquiera que sea la naturaleza de las dependencias y entidades de la administración pública. Esta revisión se ejecuta con el fin de evaluar el correcto desarrollo de las funciones de todas las áreas y unidades administrativas de dichas entidades, así como los métodos y procedimientos que regulan las actividades necesarias para cumplir con los objetivos gubernamentales, estatales o municipales; también se lleva a cabo en la aplicación y cumplimiento de presupuestos públicos, programas, normas, políticas y lineamientos que regulan la participación de los recursos de la entidad en la prestación de servicios a la sociedad.
- **Auditoría informática:** Es la revisión técnica y especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisión se realizara de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del

centro de cómputo. El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa. (Muñoz Razo, 2002)

2.7. AUDITORÍA INFORMÁTICA

2.7.1. ANTECEDENTES DE LA AUDITORÍA INFORMÁTICA

Desde que la informática se enfocó hacia el apoyo de la sistematización en las áreas del negocio, se empezaron a implantar aplicaciones administrativas como contabilidad, nomina, etc., lo cual originó lo que se conoce como auditoría de sistemas de información.

Posteriormente, cubrió las áreas de negocio en todos los niveles por medio de productos y servicios variados; proliferaron el uso de computadoras personales e irrumpieron de lleno las redes locales, la integración empresarial a través de las telecomunicaciones y un sin número de componentes de tecnología.

De este modo la tarea de los responsables de informática y los auditores de sistemas tradicionales se vio desbordada por estos acontecimientos y les imposibilitó continuar con los métodos utilizados hasta ese entonces.

Así surgió la necesidad del replanteamiento de fondo y forma de la auditoría en informática, conocida también como auditoría de sistemas, si bien esta abarca solamente la revisión de los sistemas de información en desarrollo, operación y mantenimiento, siendo éste concepto inadecuado para la auditoría en informática, ya que los elementos de informática susceptibles de revisión y control son muchos y manifiestan diversas complejidades.

En los años cuarenta empezaron a presentarse resultados relevantes en el campo de la computación, a raíz de los sistemas de apoyo para estrategias militares, posteriormente se incrementó el uso de computadoras y sus aplicaciones y se diversificó el apoyo a otros sectores de la sociedad: educación, salud, industria, política, aeronáutica, comercio, etc.

En aquellos años la seguridad y control se limitaba a proporcionar custodia física a los equipos y a permitir la utilización de los mismos a personas altamente calificadas. En las

últimas décadas, la informática se ha extendido a todas las ramas de la sociedad desde las más simples, hasta las más complejas actividades convirtiéndose en un factor determinante para obtener importantes beneficios tangibles e intangibles, pero ambos con la misma importancia para seguir impulsando la investigación y actualización constante de la tecnología.

Las empresas y organismos interesados en que la informática continúe creciendo para beneficio de la humanidad (educación, productividad, calidad, ecología, etc.) desean que este incremento se controle y oriente de manera profesional.

El incremento constante de las expectativas y necesidades relacionadas con la informática, al igual que la actualización continua de los elementos que componen la tecnología de este campo, obligan a las entidades que la aplican, a disponer de controles, políticas y procedimientos que aseguren a la alta dirección la correcta utilización de los recursos humanos, materiales, y financieros involucrados, para que se protejan adecuadamente y se orienten a la rentabilidad y competitividad de las empresas. (Hernández, 1996)

2.7.2. ALCANCE

El alcance de la auditoría define con precisión el entorno y los límites en que va a desarrollarse la auditoría informática y se complementa con los objetivos de ésta. El alcance se concretará expresamente en el informe final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas. (Vandama, Lescay, Castillo, & García, 2002)

2.7.3. DEFINICIÓN DE AUDITORÍA INFORMÁTICA

La auditoría informática es la revisión y evaluación de los controles, sistemas y procedimientos de la informática; de los equipos de cómputo, su utilización, eficiencia y seguridad; de la organización que participa en el procesamiento de la información, a fin de que por medio de señalamientos de cursos alternativos se logre una utilización más eficiente, confiable y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría informática es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza

eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. Permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes. (Kell & Zieger, 1988)

La auditoría informática es un examen exhaustivo que se realiza a las empresas con la finalidad de evaluar sus procesos, políticas y controles correspondientes al uso de los recursos informáticos ejecutados por el personal de la empresa, emitiendo un informe que contenga observaciones, recomendaciones y áreas de oportunidad para el mejoramiento y optimización permanente de la tecnología informática.

2.7.4. IMPORTANCIA DE LA AUDITORÍA INFORMÁTICA

La tecnología informática (hardware, software, redes, bases de datos, etc.) es una herramienta estratégica que brinda rentabilidad y ventajas competitivas a los negocios frente a otros negocios similares en el mercado, pero puede originar costos y desventajas si no es bien administrada por el personal encargado.

La solución clara es entonces realizar evaluaciones oportunas y completas de la función informática, a cargo de personal calificado, consultores externos, auditores en informática o evaluaciones periódicas realizadas por el mismo personal de informática

Surge entonces la obvia necesidad de auditar la función informática, ya que resulta innegable que la misma se ha convertido en una herramienta permanente y necesaria de los procesos principales de los negocios, en un aliado confiable y oportuno. Esto es posible si se implementan los controles y esquemas de seguridad requeridos para su aprovechamiento óptimo.

Una vez que la alta dirección comprenda la importancia de contar con un área independiente que asegure y promueva el buen uso y aprovechamiento de la tecnología informática, ya puede delegar la responsabilidad en personal altamente capacitado para ejercer la auditoría en informática dentro de la organización de manera formal y permanente. (Hernández, 1996)

2.7.5. OBJETIVOS DE LA AUDITORÍA INFORMÁTICA

La evaluación a los sistemas computacionales, a la administración al centro de cómputo, al desarrollo de proyectos informáticos, a la seguridad de los sistemas computacionales y a todo lo relacionado con ellos, será considerada bajo los siguientes objetivos:

- Hacer una evaluación sobre el uso de los recursos financieros en las áreas del centro de información, así como del aprovechamiento del sistema computacional, sus equipos periféricos e instalaciones.
- Evaluar el uso y aprovechamiento de los equipos de cómputo, sus periféricos, las instalaciones y mobiliario del centro de cómputo, así como el uso de sus recursos técnicos y materiales para el procesamiento de información.
- Evaluar el aprovechamiento del sistema operativo, programas, software de producción disponible.
- Evaluar el cumplimiento de planes, programas, estándares, políticas, normas y lineamientos que regulan las funciones y actividades de las áreas y de los sistemas de procesamiento de información, así como de su personal y de los usuarios del centro de información.
- Evaluar la disponibilidad de seguridades necesarias a fin de proteger y salvaguardar los equipos de tecnología disponibles para el desarrollo de actividades.
- Realizar una evaluación en el área de sistemas, con el fin de emitir un dictamen independiente sobre la razonabilidad de las operaciones del sistema y la gestión administrativa del área informática. (Muñoz Razo, 2002)

2.7.6. TIPOS DE AUDITORÍA INFORMÁTICA

La realización de las auditorías corresponde según la función de los auditores, por lo que la auditoría informática puede desarrollarse de la siguiente manera:

2.7.6.1. Según las personas que lo realizan

Se divide en dos grandes grupos estos son:

- a) **Auditoría interna:** cuando es ejecutada por auditores de las unidades de auditoría interna de las entidades y organismos del sector público y de las entidades privadas.

La unidad de auditoría interna constituye un factor importante del sistema de control interno de una entidad y como tal se constituye en un medio al servicio de la alta dirección,

destinada a salvaguardar los recursos, verificar la exactitud y veracidad de la información; promover la eficiencia y eficacia de las operaciones; estimular la observancia de las políticas y procedimientos institucionales previstos; y, el cumplimiento de las metas y objetivos programados.

Los auditores de esta unidad actuarán individual o colectivamente, con criterio independiente respecto a la operación o actividad auditada y no intervendrán en la autorización o aprobación de los procesos financieros, administrativos, operativos y ambientales, sin embargo se constituyen en asesores de la alta dirección.

b) Características de la auditoría interna

- El auditor tiene relación con la empresa.
- La relación con la empresa puede influir en la emisión del juicio sobre la evaluación de las áreas de la empresa.
- Informe para uso interno.
- Permite detectar problemas y desviaciones.
- Puede actuar periódicamente como parte de su plan anual.
- Los auditados conocen estos planes y se habitúan a las auditorías.
- Las recomendaciones habidas benefician su trabajo.

c) Auditoría Externa: Es practicada por auditores ajenos a la organización, por compañías privadas de auditoría contratadas, quienes tienen la obligación de observar la normatividad expedida al respecto en cada institución, con el objeto de emitir su opinión mediante un dictamen o informe según corresponda al tipo de auditoría que se esté llevando a efecto.

d) Características de la Auditoría Externa

- El auditor no tiene relación con la empresa.
- Revisión independiente con total libertad de criterio sin ninguna influencia
- Realizadas por despachos de auditores. (Cadena , 2011)

2.7.6.2. En función del área de tecnología de información

Se realizan de acuerdo al área o ambiente en el que se va desarrollar la auditoría, estas pueden ser las siguientes:

a) Auditoría con el computador: Es la auditoría que se realiza con el apoyo de los equipos de cómputo y sus programas para evaluar cualquier tipo de actividades y operaciones, no necesariamente computarizadas, pero sí susceptibles de ser automatizadas; dicha auditoría se realiza también a las actividades del propio centro de sistemas y a sus componentes. La principal característica de este tipo de auditoría es que, sea en un caso o en otro, o en ambos, se aprovecha el computador y sus programas para la evaluación de las actividades a revisar, de acuerdo con las necesidades concretas del auditor, utilizando en cada caso las herramientas especiales del sistema y las tradicionales de la propia auditoría.

b) Auditoría sin el computador: Es la auditoría cuyos métodos, técnicas y procedimientos están orientados únicamente a la evaluación tradicional del comportamiento y validez de las transacciones económicas, administrativas y operacionales de un área de cómputo, y en sí de todos los aspectos que afectan a las actividades en las que se utilizan sistemas informáticos, pero dicha evaluación se realiza sin el uso de los sistemas computacionales. Es también la evaluación tanto a la estructura de organización, funciones y actividades de funcionarios y personal de un centro de cómputo, así como a los perfiles de sus puestos, como de los reportes, informes y bitácoras de los sistemas, de la existencia y aplicación de planes, programas y presupuestos en dicho centro, así como del uso y aprovechamiento de los recursos informáticos para la realización de actividades, operaciones y tareas. Así mismo, es la evaluación de los sistemas de seguridad y prevención de contingencias, de la adquisición y uso del hardware, software y personal informático, y en sí de todo lo relacionado con el centro de cómputo, pero sin el uso directo de los sistemas computacionales.

c) Auditoría informática de explotación: la explotación informática se ocupa de producir resultados informáticos de todo tipo: listados impresos, ficheros soportados magnéticamente para otros informáticos, órdenes automatizadas para lanzar o modificar procesos industriales, etc.

La explotación informática se puede considerar como una fábrica con ciertas peculiaridades que la distinguen de las reales. Para realizar la explotación informática se dispone de una materia prima, los datos, que sea necesario transformar y que se sometan previamente a controles de integridad y calidad.

d) Auditoría informática de desarrollo de proyectos o aplicaciones: revisión del proceso completo de desarrollo de proyectos por parte de la empresa auditada.

El análisis se basa en cuatro aspectos:

➤ Revisión de las metodologías utilizadas.

- Control interno de las aplicaciones.
- Satisfacción de usuarios.
- Control de procesos y ejecuciones de programas críticos.

e) Auditoría de seguridad informática: Es la revisión exhaustiva, técnica y especializada que se realiza a todo lo relacionado con la seguridad de un sistema de cómputo sus áreas y personal, así como a las actividades, funciones y acciones preventivas y correctivas que contribuyan a salvaguardar la seguridad de los equipos computacionales, las bases de datos, redes, instalaciones y usuarios del sistema. Es también la revisión de los planes de contingencia y medidas de protección para la información, los usuarios y los propios sistemas computacionales, y en sí para todos aquellos aspectos que contribuyen a la protección y salvaguarda en el buen funcionamiento del área de sistematización, sistemas de redes o computadores personales, incluyendo la prevención y erradicación de los virus informáticos.

f) Auditoría a los sistemas de redes: Es la revisión exhaustiva, específica y especializada que se realiza a los sistemas de redes de una empresa, considerando en la evaluación los tipos de redes, arquitectura, topología, sus protocolos de comunicación, las conexiones, accesos, privilegios, administración y demás aspectos que repercuten en su instalación, administración, funcionamiento y aprovechamiento. Es también la revisión del software institucional, de los recursos informáticos e información de las operaciones, actividades y funciones que permiten compartir las bases de datos, instalaciones, software y hardware de un sistema de red.

g) Auditoría integral a los centros de cómputo: Es la revisión exhaustiva, sistemática y global que se realiza por medio de un equipo multidisciplinario de auditores, de todas las actividades y operaciones de un centro de sistematización, a fin de evaluar, en forma integral, el uso adecuado de sus sistemas de cómputo, equipos periféricos y de apoyo para el procesamiento de información de la empresa, así como de la red de servicios de una empresa y el desarrollo correcto de las funciones de sus áreas, personal y usuarios. Es también la revisión de la administración del sistema, del manejo y control de los sistemas operativos, lenguajes, programas y paqueterías de aplicación, así como de la administración y control de proyectos, la adquisición del hardware y software institucionales, de la adecuada integración y uso de sus recursos informáticos y de la existencia y cumplimiento de las normas, políticas, estándares y procedimientos que regulan la actuación del sistema, del personal y usuarios del centro de cómputo. Todo está hecho de manera global por medio de un equipo multidisciplinario de auditores.

h) Auditoría Outsourcing: Es la revisión exhaustiva, sistemática y especializada que se realiza para evaluar la calidad en el servicio de asesoría o procesamiento externo de información que proporciona una empresa a otra. Esto se lleva a cabo con el fin de revisar la confiabilidad, oportunidad, suficiencia y asesoría por parte de los prestadores de servicios de procesamiento de datos, así como el cumplimiento de las funciones y actividades que tienen encomendados los prestadores de servicios, usuarios y el personal en general. Dicha revisión se realiza también en los equipos y sistemas.

i) Auditoría ergonómica de sistemas computacionales: Es la revisión técnica, específica y especializada que se realiza para evaluar la calidad, eficiencia y utilidad del entorno hombre-máquina-medio ambiente que rodea el uso de sistemas computacionales en una empresa. Esta revisión se realiza también con el propósito de evaluar la correcta adquisición y uso del mobiliario, equipo y sistemas, a fin de proporcionar el bienestar, confort y comodidad que requieren los usuarios de los sistemas de cómputo de la empresa, así como evaluar la detección de los posibles problemas y sus repercusiones, y la determinación de las soluciones relacionadas con la salud física y bienestar de los usuarios de los sistemas de la empresa. (Muñoz Razo, 2002)

2.8. CONTROL INTERNO INFORMÁTICO

El control interno informático controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procesamientos, estándares y normas fijadas por la dirección de la organización y/o dirección informática, así como los requerimientos legales.

La misión del control interno informático es asegurarse de que las medidas que se obtienen de los mecanismos implantados por cada responsable sean correctas y válidas.

2.8.1. OBJETIVOS DEL CONTROL INTERNO INFORMÁTICO

- a)** Controlar que las actividades se realicen cumpliendo con los procedimientos y normas fijadas.
- b)** Salvaguardar los activos contribuyendo a la protección del hardware, software y recursos humanos.
- c)** Mantener la Integridad de datos su consistencia y que no exista duplicidad.
- d)** Colaborar y apoyar el trabajo de auditoría informática, así como de las auditorías externas al grupo.

- e) Definir, implantar, ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio informático.
- f) Garantizar la seguridad y confidencialidad en el área informática.

2.8.2. TIPOS DE CONTROLES INTERNOS

En el ambiente informático, el control interno se materializa fundamentalmente en controles de tres tipos:

1. **Controles preventivos:** Para tratar de evitar la producción de errores o hechos fraudulentos, como por ejemplo el software de seguridad que evita el acceso a personal no autorizado.
2. **Controles detectivos:** Tratan de descubrir posteriores errores o fraudes que no haya sido posible evitarlos con controles preventivos.
3. **Controles correctivos:** Tratan de asegurar que se corrijan todos los errores identificados mediante los controles detectivos. Facilitan la vuelta a la normalidad cuando se hayan producido incidencias. (Piattini del Peso, 2005)

2.9. PROCESO DE AUDITORÍA INFORMÁTICA

A continuación se mencionan las fases o pasos que pueden ser aplicables para cualquier tipo de auditoría dentro del campo informático.

Tabla 3: Proceso de Auditoría Informática

FASE	ACTUACIONES RELEVANTES DEL AUDITOR
1. Planeación de la auditoría	<ul style="list-style-type: none"> ➤ Recopilación de información general de la entidad tales como: <ul style="list-style-type: none"> - Como se encuentran distribuidos los sistemas en el área. - Como y de qué tipo son los equipos que están instalados en el centro de sistemas. ➤ Establecer los objetivos de la auditoría. ➤ Determinar los puntos que serán evaluados en la auditoría. ➤ Elaborar planes, programas y presupuestos para realizar la auditoría. ➤ Identificar y seleccionar los métodos, procedimientos y herramientas necesarias para la auditoría. ➤ Realizar una evaluación preliminar del sistema de control interno, área informática.
2. Ejecución de la auditoría informática	<ul style="list-style-type: none"> ➤ Aplicar los instrumentos y herramientas para la auditoría. ➤ Asignar los recursos y actividades conforme a los planes y programas. ➤ Recopilar la documentación y evidencia de la auditoría. ➤ Identificar y elaborar documentos de desviaciones. ➤ Integrar los documentos y papeles de trabajo. ➤ Elaborar el borrador de desviaciones.
3. Informe de auditoría	<ul style="list-style-type: none"> ➤ Comentar las situaciones encontradas con los auditados encontrar, conjuntamente con los auditados, las causas de las desviaciones y posibles soluciones. ➤ Analizar, depurar y corregir las desviaciones encontradas jerarquizar las desviaciones encontradas y concentrar las más importantes. ➤ Comentar las situaciones relevantes con los directivos del

	<p>área de sistemas y confirmar las causas y soluciones.</p> <ul style="list-style-type: none"> ➤ Concentrar, depurar y elaborar el informe final de auditoría. ➤ Presentar el informe.
--	---

Fuente: Libro Auditoría en Sistemas Informáticos.²

Elaborado por: Autor de Tesis.

a) Planificación de la Auditoría Informática:

La etapa de planificación es una de las más importantes dentro del proceso de auditoría debido a que se define las actividades que se van a desarrollar en el transcurso de la misma, así como las técnicas, procedimientos y programas necesarios para llevar a cabo la fase de ejecución y de esta forma poder obtener información que respalde el dictamen de auditoría.

b) Ejecución de la auditoría:

Concretamente, se tiene lo siguiente:

- Realizar las acciones programadas para la auditoría.
- Aplicar los instrumentos y herramientas para la auditoría.
- Identificar y elaborar los hallazgos de auditoría.
- Elaborar el dictamen de auditoría y presentarlo a discusión

c) Informes de auditoría:

En el informe de auditoría se reportan las situaciones encontradas durante la evaluación, pero también se deben incluir las causas que originan esas situaciones y las posibles sugerencias para solucionar los problemas encontrados.

Está claro que el producto final y el más importante de una auditoría informática es la elaboración correcta del informe, ya que en éste se presentan los resultados obtenidos durante la evaluación de la gestión administrativa del centro de cómputo, o de cualquier otro aspecto relacionada con los sistemas.

El procedimiento para elaboración de dicho informe se compone de los siguientes pasos:

- Aplicar instrumentos de recopilación.
- Registrar las desviaciones halladas durante la revisión.
- Comentar las situaciones encontradas con los auditores.

². MUNOZ, Carlos. (2002) c. *Auditoría en Sistemas Informáticos* (Pág. 185 -235-274). México: Editorial Cámara Nacional de la Industria Editorial Mexicana.

- Encontrar, conjuntamente con los auditados, las causas de las desviaciones y sus posibles soluciones.
- Analizar, depurar y corregir las desviaciones encontradas.
- Jerarquizar las desviaciones encontradas y concentrar las más importantes.
- Comentar las situaciones relevantes con los directivos del área informática y confirmar las causas y soluciones.
- Concentrar, depurar y elaborar el informe final de auditoría, así como el informe del auditor.
- Presentar el informe a los directivos de la institución. (Piattini & Del Peso, 2005)

2.10. INSTRUMENTOS DE RECOPIACIÓN EN LA AUDITORÍA INFORMÁTICA

Estos sirven para hacer una evaluación correcta del funcionamiento del área de sistemas, de la operación del propio sistema o de su gestión informática, beneficiándose con ello debido a la ya probada eficiencia y eficacia, en las cuales se ha conseguido buenos resultados.

Tabla 4: Instrumentos de Recopilación en la Auditoría Informática

INSTRUMENTOS DE RECOPIACIÓN EN LA AUDITORÍA INFORMÁTICA	
Técnicas, herramientas y métodos útiles en la recopilación de la información para la auditoría de sistemas.	<ul style="list-style-type: none"> ➤ Entrevistas. ➤ Cuestionarios. ➤ Encuestas. ➤ Observación. ➤ Inventarios. ➤ Muestreo. ➤ Experimentación.
Técnicas, métodos y procedimientos especializados para la evaluación de sistemas computacionales.	<ul style="list-style-type: none"> ➤ Examen. ➤ Inspección. ➤ Confirmación. ➤ Comparación. ➤ Revisión documental. ➤ Acta testimonial.

	<ul style="list-style-type: none"> ➤ Matriz de evaluación. ➤ Matriz DOFA
Técnicas, métodos y procedimientos de apoyo para emitir los diagnósticos sobre los sistemas computacionales.	<ul style="list-style-type: none"> ➤ Guías de evaluación. ➤ Ponderación. ➤ Modelos de simulación. ➤ Evaluación. ➤ Diagrama del círculo de evaluación. ➤ Lista de verificación. ➤ Análisis de la diagramación de sistemas. ➤ Diagramas de seguimiento de la auditoría. ➤ Programas para revisión por computadoras.

Fuente: Libro Auditoría en Sistemas Informáticos.³

Elaborado por: Autor de Tesis.

³. MUNOZ, Carlos. (2002) d. *Auditoría en Sistemas Informáticos* (Pág. 47 y 48). México: Editorial Cámara Nacional de la Industria Editorial Mexicana.

2.11. PAPELES DE TRABAJO

En una auditoría de sistemas, los papeles de trabajo representan el sustento para registrar los datos e información que se van recolectando durante la evaluación, sirven para mantener el sentido e importancia de las desviaciones encontradas durante la revisión, así como para establecer las posibles causas de las desviaciones y para proponer las probables soluciones que reporta como parte de su trabajo.

Los papeles de trabajo se deben diseñar y organizar según las circunstancias y las necesidades del auditor. Estos han de ser claros y concisos. Todo el trabajo de auditoría debe quedar reflejado en papeles de trabajo por los siguientes motivos:

- Recogen la evidencia obtenida a lo largo del trabajo.
- Ayudan al auditor en el desarrollo de su trabajo.
- Ofrecen un soporte del trabajo realizado para, así, poder utilizarlo en auditorías sucesivas y pueda ser revisado por terceros.

A continuación se presenta una propuesta para integrar estos papeles:

- Hoja de identificación.
- Índice de contenido de los papeles de trabajo.
- Dictamen preliminar (borrador).
- Resumen de desviaciones detectadas (las más importantes).
- Situaciones encontradas (Situaciones causas y soluciones).
- Programa de trabajo de auditoría.
- Guía de auditoría.
- Inventario de software.
- Inventario de hardware.
- Inventario de consumibles.
- Manual de organización.
- Descripción de puestos.
- Reportes de pruebas y resultados.
- RespalDOS de datos.
- RespalDOS de las bases de datos y de los sistemas.
- Guías de claves para el señalamiento de los papeles de trabajo.
- Cuadros y estadísticas concentradores de investigación.

- Anexos de recopilación de información.
- Diagramas de flujo, de programas y de desarrollo de sistemas.
- Testimoniales, actas, y documentos legales de comprobación y confirmación. (Muñoz Razo, 2002)

2.12. PROGRAMAS DE AUDITORÍA

Un programa de auditoría es un conjunto documentado de procedimientos diseñados para alcanzar los objetivos de auditoría planificados. El esquema típico de un programa de auditoría incluye lo siguiente:

- a. Tema de auditoría:** Donde se identifica el área a ser auditada.
- b. Objetivos de auditoría:** Donde se indica el propósito del trabajo de auditoría a realizar.
- c. Alcances de auditoría:** Aquí se identifica los sistemas específicos o unidades de organización que se han de incluir en la revisión en un período de tiempo determinado.
- d. Planificación previa:** Donde se identifica los recursos y destrezas que se necesitan para realizar el trabajo así como las fuentes de información para pruebas o revisión y lugares físicos o instalaciones donde se va auditar.
- e. Procedimientos de auditoría para:**
 - Recopilación de datos.
 - Identificación de listas de personas a entrevistar.
 - Identificación y selección del enfoque del trabajo.
 - Identificación y obtención de políticas, normas y directivas.
 - Desarrollo de herramientas y metodología para probar y verificar los controles existentes.
 - Procedimientos para evaluar los resultados de las pruebas y revisiones.
 - Procedimientos de comunicación con la gerencia.
 - Procedimientos de seguimiento.

El programa de auditoría se convierte también en una guía para documentar los diversos pasos de auditoría y para señalar la ubicación del material de evidencia.

Generalmente tiene la siguiente estructura: (Monografias.com, Estructura del Programa de Auditoría, 2009)

Tabla 5: Estructura del Programa de Auditoría

PROCEDIMIENTOS DE AUDITORÍA	LUGAR	PAPELES DE TRABAJO	HECHO POR:

Los procedimientos involucran pruebas de cumplimiento o pruebas sustantivas, las de cumplimiento se hacen para verificar que los controles funcionan de acuerdo a las políticas y procedimientos establecidos y las pruebas sustantivas verifican si los controles establecidos por las políticas o procedimientos son eficaces.

2.12.1. CARACTERÍSTICAS DEL PROGRAMA DE AUDITORÍA

El programa de auditoría contiene las actividades que se llevarán a cabo en la auditoría, por ello; su elaboración debe ser óptima y su autor debe tener conocimiento de todos los aspectos que abarcará el trabajo y las actividades que se deben realizar.

El programa debe ser además flexible, y no debe tomar en cuenta aspectos poco relevantes que capten, de manera innecesaria, recursos que puedan destinarse a la evaluación de aspectos importantes.

Entre las características que debe tener el programa de auditoría, podemos anotar:

- Debe ser sencillo y comprensivo.
- Debe ser elaborado tomando en cuenta los procedimientos que se utilizarán de acuerdo al tipo de empresa a examinar.
- El programa debe estar encaminado a alcanzar el objetivo principal.
- Debe desecharse los procedimientos excesivos o de repetición.
- El programa debe permitir al auditor a examinar, analizar, investigar, obtener evidencias para luego poder dictaminar y recomendar.
- Las sociedades auditoras, acostumbran tener formatos preestablecidos los cuales deben ser flexibles para que puedan ser adecuados a un determinado tipo de empresa.

- El programa debe ser confeccionado en forma actualizada y con amplio sentido crítico de parte del auditor.

2.12.2. CLASIFICACIÓN DE LOS PROGRAMAS DE AUDITORÍA

De acuerdo a su profundidad y extensión, existen dos tipos de programas de auditoría, que son:

- **Programas de auditoría generales:** son los que se limitan a enunciar de forma genérica las técnicas a aplicarse y los objetivos trazados. Generalmente se destinan al jefe del equipo de auditoría.
- **Programa de Auditoría Detallados:** son los que describen de forma minuciosa y práctica los procedimientos y técnicas a aplicarse. Van destinados a los integrantes del equipo de auditoría. (Ortiz & Ortiz, 2002)

2.13. HALLAZGOS DE AUDITORÍA.

Se considera que los hallazgos en auditoría son las diferencias significativas encontradas en el trabajo de auditoría con relación a lo normado o a lo presentado por la gerencia.

Atributos del hallazgo:

- **Condición:** La realidad encontrada
- **Criterio:** Cómo debe ser (la norma, la ley, el reglamento, lo que debe ser).
- **Causa:** Qué originó la diferencia encontrada.
- **Efecto:** Qué efectos puede ocasionar la diferencia encontrada.

Al plasmar el hallazgo el auditor primeramente indicará el título del hallazgo, luego los atributos, a continuación indicarán la opinión de las personas auditadas sobre el hallazgo encontrado, posteriormente indicarán su conclusión sobre el hallazgo y finalmente hará las recomendaciones pertinentes. Es conveniente que los hallazgos sean presentados en hojas individuales.

Solamente las diferencias significativas encontradas se pueden considerar como hallazgos (generalmente determinadas por la materialidad), aunque en el sector público se deben dar a conocer todas las diferencias, aun no siendo significativas.

Una vez concluida la fase de ejecución, se debe solicitar la carta de salvaguarda o carta de gerencia, donde la gerencia de la empresa auditada da a conocer que se han entregado todos los documentos que oportunamente fueron solicitados. (Ximénez, 2011)

2.14. MARCAS DE AUDITORÍA

Las marcas de auditoría son signos o símbolos convencionales que utiliza el auditor, para identificar el tipo de procedimiento, tarea o pruebas realizadas en la ejecución de un examen. El uso de marcas simples facilita su entendimiento.

Se recomienda la utilización de marcas estándar, entre las que se señala las siguientes:

Tabla 6: Marcas de Auditoría

MARCAS	SIGNIFICADO
✓	Verificado mediante inspección física.
@	Analizado.
↔	Comparado.
⇒	Determinación de hallazgo.
∝	Cotejado con inventarios.
⊗	Incluir en informe.
≍	Cotejado con documentos.
S	Documentación sustentatoria.
^	Transacción rastreada.
Σ	Comprobado sumas.
C	Circularizado.
℄	Confirmado.
N	No autorizado.

Fuente: Curiel, Auditoría de Estados Financieros

Elaborado por: Autor de Tesis

2.15. COMUNICACIÓN DE RESULTADOS DE AUDITORÍA

Es muy importante que el auditor mantenga una comunicación continua y constante con los funcionarios y empleados relacionados con el examen, con el propósito de mantenerles informados sobre las deficiencias y desviaciones detectadas a fin de que en forma oportuna se presente los justificativos o se tomen las acciones correctivas pertinentes.

La comunicación de resultados es la última fase del proceso de la auditoría, sin embargo ésta se cumple durante la ejecución del examen.

Está dirigida a los funcionarios de la entidad examinada con el propósito de que presenten la información verbal o escrita respecto a los asuntos observados.

Esta fase comprende también, la redacción y revisión final del borrador del informe, que será elaborado en el transcurso del examen, con el fin de que al finalizar el trabajo en el campo y previa convocatoria, se comunique los resultados mediante su lectura a las autoridades, funcionarios y exfuncionarios responsables de las operaciones examinadas.

El informe contendrá los comentarios, conclusiones y recomendaciones relativos a los hallazgos de auditoría. (Caneda, 2011)

2.16. NORMAS DE CONTROL INTERNO PARA LA AUDITORÍA INFORMÁTICA⁴

La Contraloría General del Estado, establece Normas de Control Interno, para proveer a las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, de un importante marco normativo a través del cual puedan desarrollarse para alcanzar sus objetivos y maximizar los servicios públicos que deben proporcionar a la comunidad.

A continuación se describe de forma general las normas emitidas por la contraloría general del Estado:

Las normas emitidas por la CGE son:

100.- Normas generales.

200.- Ambiente del control.

300.- Evaluación de riesgos.

400.- Actividades de control.

401.- Generales.

402.- Administración financiera – PRESUPUESTO.

⁴CONTRALORÍA GENERAL DEL ESTADO ECUATORIANO(2009)Normas de Control Interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos

- 403.-** Administración financiera – TESORERÍA.
- 404.-** Administración financiera – DEUDA PÚBLICA
- 405.-** Administración financiera – CONTABILIDAD GUBERNAMENTAL.
- 406.-** Administración financiera – ADMINISTRACIÓN DE BIENES.
- 407.-** Administración del talento humano.
- 408.-** Administración de proyectos.
- 409.-** Gestión ambiental.
- 410.- Tecnología de la información.**
- 500.-** Información y comunicación.
- 600.-** Seguimiento.

En el grupo 400, subgrupo 410 y en el grupo 500, se encuentran las normas para la evaluación del control interno en el área de la Informática.

A continuación se describe las normas correspondientes a la Tecnología de la información:

410.- Tecnología de la información

Tabla 7 Normas de Tecnología de la información

TECNOLOGÍA DE LA INFORMACIÓN	
410-01	Organización informática.
410-02	Segregación de funciones.
410-03	Plan informático estratégico de tecnología.
410-04	Políticas y procedimientos.
410-05	Modelo de información organizacional.
410-06	Administración de proyectos tecnológicos.
410-07	Desarrollo y adquisición de software aplicativo.
410-08	Adquisiciones de infraestructura tecnológica.
410-09	Mantenimiento y control de la infraestructura tecnológica.

410-10	Seguridad de tecnología de la información.
410-11	Plan de contingencias.
410-12	Administración de soporte de tecnología de información.
410-13	Monitoreo y evaluación de los procesos y servicios.
410-14	Sitio web, servicios de internet e intranet.
410-15	Capacitación informática.
410-16	Comité informático.
410-17	Firmas electrónicas.
INFORMACIÓN Y COMUNICACIÓN	
500-01	Controles sobre sistemas de información.
500-02	Canales de comunicación abiertos.

Fuente: Normas de Control Interno

Elaborado por: Autor de Tesis

CAPÍTULO III

3. DIAGNÓSTICO SITUACIONAL DEL INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS (IECE) REGIONAL 3 RIOBAMBA

3.1. DIAGNÓSTICO SITUACIONAL

Previo al análisis FODA al IECE Regional 3 Riobamba, se hizo un reconocimiento dentro de la entidad de toda la información que nos daría la base para realizar este análisis, el mismo que se obtuvo mediante la aplicación de encuestas a: funcionarios de la entidad, y permite realizar una comparación entre las perspectivas que tienen cada uno de ellos para determinar el diagnóstico situacional basado en fortalezas, oportunidades, debilidades y amenazas. (Ver anexo 1)

3.2. ANÁLISIS FODA

El análisis FODA consiste en identificar las fortalezas, oportunidades, debilidades y amenazas para de esta forma aprovechar de la mejor manera las fortalezas y oportunidades que se presenten en el análisis y tratando de disminuir al máximo las debilidades y amenazas que se presentan para de esta forma mantener un adecuado sistema de control interno.

3.2.1. MATRIZ FODA

Tabla 8: Matriz FODA

FACTORES INTERNOS CLAVES	FACTORES EXTERNOS CLAVES
FORTALEZAS	OPORTUNIDADES
<ul style="list-style-type: none">➤ Cobertura a nivel nacional.➤ Entidad financiera del sector público con patrimonio e ingresos propios.➤ Posición sólida en el mercado.➤ Talento humano con conocimientos idóneos.➤ Firmas de convenios y acuerdos.➤ Adecuado ambiente de trabajo de la unidad de TICs.➤ Participación del personal involucrado al momento de establecer necesidades de la unidad de TICs.➤ Información interna protegida.	<ul style="list-style-type: none">➤ Demanda de crédito educativo y becas.➤ Confianza de clientes hacia el IECE.➤ Adquisición de nuevas tecnologías.➤ La educación es objetivo estratégico dentro del Plan Nacional de Desarrollo.➤ Cooperación internacional – APICE.

DEBILIDADES	AMENAZAS
<ul style="list-style-type: none"> ➤ Ausencia de procesos documentados, normatividad desactualizada y falta de manuales de procedimiento. ➤ El inadecuado manejo del archivo de documentos. ➤ La comunicación interna y externa es deficiente. ➤ La cartera vencida. ➤ Falta de seguimiento continuo en procesos de capacitación al personal. ➤ No cuenta con personal suficiente en la unidad de TICs. ➤ La unidad de TICs no cuenta con un modelo de información organizacional. ➤ El servicio de internet es regular. ➤ Las medidas de seguridad no son apropiadas para evitar la pérdida o sustracción de los recursos informáticos en las diferentes unidades. 	<ul style="list-style-type: none"> ➤ Los beneficiarios del crédito no tendrían acceso al mercado laboral, lo que incide en la capacidad de pago del crédito. ➤ La crisis mundial se ve reflejada en una disminución de la oferta de becas internacionales. ➤ Recortes del presupuesto del estado. ➤ Creciente competencia del sector privado con el financiamiento del crédito. ➤ Cambio en las políticas del estado que afecten a la institución.

Fuente: Investigación

Elaborado por: Autor de Tesis

3.2.2. ANÁLISIS DE MEDIOS INTERNOS

Se entiende por medio interno a todas las relaciones y actividades que se harán al interior de la organización lo cual se realiza mediante un análisis exhaustivo en el desarrollo de sus funciones en términos de gestión administrativa.

El análisis de medio interno conocido también como diagnóstico permite interpretar la situación de la institución, establecer la relación causa y efecto y concluir en una síntesis de puntos sólidos y problemas.

El análisis de medio interno constituye una evaluación de la organización cuyo objetivo es identificar fortalezas (logros) y debilidades (problemas). Se empieza indagando como están actualmente los elementos más importantes de la organización, como son la visión, misión y los grandes objetivos y políticas institucionales.

- **Fortalezas:** Son aquellos factores en los cuales la empresa ha conseguido logros y posee ventajas competitivas en todas las áreas de su competencia.
- **Debilidades:** Son aquellos factores que provocan vulnerabilidad y desventajas para la empresa.

Tabla 9: Análisis de medios internos

CÓDIGO	ASPECTOS INTERNOS	JUSTIFICACIÓN
FORTALEZAS		
F1	Cobertura a nivel nacional	El IECE cuenta con agencias en todo el territorio nacional.
F2	Entidad financiera del sector público con patrimonio e ingresos propios.	Los fondos provienen de entidades públicas y privadas del Ecuador y de gobiernos de países amigos y organismos internacionales.
F3	Posición sólida en el mercado	Credibilidad y confianza de los clientes.
F4	Talento humano con conocimientos idóneos.	Personal profesional en las distintas unidades de la institución.
F5	Firmas de convenios y acuerdos.	Cuenta con el convenio marco de cooperación interinstitucional con la SENESCYT, convenios con países amigos como Cuba, Brasil, Rusia etc.
F6	Adecuado ambiente de trabajo en la unidad de TICs.	Permite cumplir con las actividades atribuidas a la unidad de TICs.
F7	Participación del personal involucrado al momento de establecer necesidades de la unidad de TICs.	Participación de gerencia y jefes departamentales.

F8	Información interna protegida.	La información interna está protegida contra posible sabotajes ocasionadas por personas ajenas a la institución.
F9	Claves de acceso asignado por las autoridades de la institución.	Las claves de acceso son asignadas por las autoridades de la institución y se realiza cambios periódicos por motivos de seguridad.
DEBILIDADES		
D1	Ausencia de procesos documentados, normatividad desactualizada y falta de manuales de procedimiento.	Causa procesos lentos por no contar con manuales adecuados.
D2	Inexistencia de una unidad encargada específicamente de la administración de bienes.	No cuenta con una unidad que se encargue de manera específica de la administración de los bienes que posee.
D3	El inadecuado manejo del archivo de documentos.	El archivo de documentos no se lo realiza de manera adecuada, dificultando su localización oportuna.
D4	La comunicación interna y externa es deficiente.	No cuenta con líneas de comunicación adecuadas.
D5	Problemas en la recuperación de cartera.	No se está llevando a cabo un análisis de crédito ni se está cumpliendo con parámetros, establecidos en la firma del contrato.

D6	Falta de seguimiento continuo en procesos de capacitación al personal.	No se realiza una capacitación completa al personal en temas relacionados a sus áreas.
D7	No cuenta con personal suficiente en la unidad de TICs.	La institución no cuenta con personal suficiente para realizar las actividades en la unidad de TICs.
D8	La unidad de TICs no cuenta con un modelo de información organizacional.	La unidad de TICs no dispone de un modelo de información organizacional adaptado a sus procesos y procedimientos.
D9	El servicio de internet es regular.	El servicio de internet no satisface las necesidades de los funcionarios.
D10	Las medidas de seguridad no son apropiadas para evitar la pérdida o sustracción de los recursos informáticos en las diferentes unidades.	Las medidas de seguridad adoptadas en las diferentes áreas de la institución no son las adecuadas y existe vulnerabilidad en su cuidado.

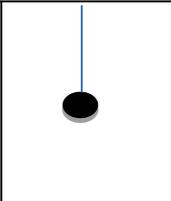
Fuente: Investigación

Elaborado por: Autor de Tesis

PERFIL ESTRATÉGICO INTERNO

Tabla 10: Perfil Estratégico Interno

ASPECTOS INTERNOS		CLASIFICACIÓN DE IMPACTO				
		DEBILIDADES		NORMAL	FORTALEZAS	
		GRAN DEBILIDAD	DEBILIDAD	EQUILIBRIO	FORTALEZA	GRAN FORTALEZA
		1	2	3	4	5
F1	Cobertura a nivel nacional.					●
F2	Entidad financiera del sector público con patrimonio e ingresos propios.					●
F3	Posición sólida en el mercado.					●
F4	Talento humano con conocimientos idóneos.					●
F5	Firmas de convenios y acuerdos.					●
F6	Adecuado ambiente de trabajo del área de TICs.					●
F7	Participación del personal involucrado al momento de establecer necesidades del área de TICs.				●	
F8	Información interna protegida.				●	
F9	Claves de acceso asignado por las autoridades de la institución.					●
D1	Ausencia de procesos documentados, normatividad desactualizada y falta de manuales de procedimiento.	●				
D3	Inadecuado manejo del archivo de documentos.		●			
D4	La comunicación interna y externa es deficiente.		●			
D5	La cartera vencida	●				
D6	Falta de seguimiento continuo en procesos de capacitación al personal.		●			
D7	No cuenta con personal suficiente en el área de TICs.		●			
D8	No cuenta con un modelo de información organizacional.	●				
D9	El servicio de internet es regular.		●			

D10	Las medidas de seguridad no son apropiadas para evitar la pérdida o sustracción de los recursos informáticos en diferentes áreas.					
TOTAL	18	3	6	0	2	7
PORCENTAJE	100%	16,67%	33,33%	0	11,11%	38,89%

Fuente: Investigación

Elaborado por: Autor de Tesis

Para la evaluación del desenvolvimiento de la organización la ponderación será la siguiente: Cada factor tendrá una ponderación, la misma que fluctuara de 0 hasta 1 por lo que la suma será igual a 1.

La clasificación que se usara en los parámetros será:

1. = debilidad grave o muy importante
2. = debilidad menor
3. = equilibrio
4. = fortaleza menor
5. = fortaleza importante

El resultado ponderado se obtiene entre la ponderación y el parámetro asignado. Se suma el resultado ponderado de cada uno de los factores.

Para resultados internos la calificación puede ser 5 máximo que implica que la entidad está estable y 1 mínimo que indica que tiene problemas. Cuando el resultado es inferior al promedio se tienen más debilidades que fortalezas, y si el resultado es mayor al promedio se poseen más fortalezas que debilidades. (Fred, 1997)

PONDERACIÓN PERFIL ESTRATÉGICO INTERNO

Tabla 11: Ponderación Perfil Estratégico Interno

Nº	FACTORES INTERNOS CLAVES	PONDERACIÓN	CLASIFICACIÓN	RESULTADO PONDERADO
FORTALEZAS				
1	Cobertura a nivel nacional.	0,056	5	0,28
2	Entidad financiera del sector público con patrimonio e ingresos propios.	0,056	5	0,28
3	Posición sólida en el mercado.	0,056	5	0,28
4	Talento humano con conocimientos idóneos.	0,056	5	0,28
5	Firmas de convenios y acuerdos.	0,056	5	0,28
6	Adecuado ambiente de trabajo del área de TICs.	0,056	5	0,28
7	Participación del personal involucrado al momento de establecer necesidades del área de TICs.	0,056	4	0,22
8	Información interna protegida	0,056	4	0,22
9	Claves de acceso asignado por las autoridades de la institución.	0,056	5	0,28
DEBILIDADES				
10	Ausencia de procesos documentados, normatividad desactualizada y falta de manuales de procedimiento.	0,056	1	0,06
11	El inadecuado manejo del archivo de documentos.	0,056	2	0,11
12	La comunicación interna y externa es deficiente.	0,056	2	0,11
13	La cartera vencida.	0,056	1	0,06
14	Falta de seguimiento continuo en procesos de capacitación al personal.	0,056	2	0,11
15	No cuenta con personal suficiente en la unidad de TICs.	0,056	2	0,11

16	No cuenta con un modelo de información organizacional	0,056	1	0,06
17	El servicio de internet es regular.	0,056	2	0,11
18	Las medidas de seguridad no son apropiadas para evitar la pérdida o sustracción de los recursos informáticos en diferentes unidades.	0,056	2	0,11
TOTAL		1,00	58	3,22

Fuente: Investigación

Elaborado por: Autor de Tesis

Análisis: El resultado de 3,22 indica que la institución se encuentra en equilibrio en cuanto a fortalezas y debilidades por lo que se debe aprovechar las fortalezas como es; la posición sólida que tiene en mercado, los convenios de cooperación interinstitucional con la SENESCYT, convenios con países amigos como Cuba, Brasil, Rusia etc., la participación de personal que se reúne para identificar las necesidades de tecnología a través del plan anual de contrataciones, el contar con el técnico informático con conocimiento y experiencia para realizar sus actividades y solucionar problemas cuando lo amerite, el brindar mantenimiento preventivo y correctivo a los equipos que están disponibles en la institución, y contar con un adecuado ambiente de trabajo lo cual permite cumplir con las actividades encomendadas.

Entre las debilidades encontradas y las cuales se deben mejorar se encuentra la inadecuada implementación de procesos documentados; realizar un análisis exhaustivo de la cartera vencida para determinar el retraso en el cumplimiento de las obligaciones de pago, desde la menos riesgosa pasando por la cartera ya litigiosa y constatar las cuentas incobrables, así mismo es urgente el seguimiento continuo en procesos de capacitación, es importante que las autoridades evalúen y consideren la necesidad de contratar otro funcionario que labore con el funcionario de la unidad de TICs, elaborar un modelo de información organizacional, mejorar el servicio de internet de tal manera que permita el correcto desenvolvimiento de las actividades en el Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba.

3.2.3. ANÁLISIS DE MEDIOS EXTERNOS

Se refiere a la identificación de los factores exógenos, más allá de la organización, que condicionan su desempeño, tanto en sus aspectos positivos (oportunidades), como negativos (amenazas).

La evolución económica del país, su crecimiento y desarrollo, las relaciones internacionales, los tratados de comercio.

Los cambios demográficos y culturales que alteran los niveles de demanda. El desarrollo tecnológico y los avances científicos que la organización debería conocer y eventualmente adoptar. El riesgo de factores naturales (clima, terremotos, inundaciones, sequía). Aspectos políticos y legales, etc.

- **Oportunidades:** Son aquellos factores externos a la organización que están ocurriendo o que podrán ocurrir en el futuro y que la institución puede aprovechar para obtener ventajas competitivas que cooperan al logro de los objetivos y al desarrollo de la empresa.
- **Amenazas:** Son aquellos factores que están ocurriendo o que podrán ocurrir en el futuro, que pueden afectar desfavorablemente y en forma relevante el logro de los objetivos y debemos neutralizarlos.

Tabla 12: Análisis de Medio Externo

CÓDIGO	ASPECTOS EXTERNOS	JUSTIFICACIÓN
OPORTUNIDADES		
O1	Demanda de crédito educativo y becas.	Demanda elevada de clientes para ser beneficiarios del crédito educativo y becas.
O2	Confianza de clientes hacia el IECE.	Preferencia de los clientes hacia el IECE, existiendo otras instituciones financieras.

O3	Adquisición de nuevas tecnologías para la institución.	En el mercado existen alternativas informáticas como hardware y software que deberían ser adquiridas para mejorar el servicio prestado por las entidades públicas.
O4	La educación es objetivo estratégico dentro del Plan Nacional de Desarrollo.	El Plan Nacional de Desarrollo entre sus 12 objetivos menciona 2 que son: Mejorar las capacidades y potencialidades de la ciudadanía; y, Garantizar el trabajo estable, justo y digno, que a través del IECE propenderá a cumplir los mismos.
O5	Cooperación internacional – APICE	La Asociación Panamericana de Instituciones de Crédito Educativo – APICE permite ampliar los horizontes del IECE y constituye una gran oportunidad para los clientes.
AMENAZAS		
A1	Los beneficiarios del crédito no tendrían acceso al mercado laboral, lo que incide en la capacidad de pago del crédito.	El desempleo es un factor crítico en nuestro país, que causa que los estudiantes luego de culminar su carrera no cuenten con el dinero para cancelar su deuda.
A2	La crisis mundial se ve reflejada en una disminución de la oferta de becas internacionales.	Las ofertas de becas internacionales se complican con la crisis mundial, debido a que se incrementan los costos para realizar las mismas.

<p>A3</p>	<p>Recortes del presupuesto del estado.</p>	<p>En los últimos años se ha recibido una gran ayuda por parte del estado por que un recorte en el presupuesto no permitiría cumplir con los objetivos plantados por la institución.</p>
<p>A4</p>	<p>Creciente competencia del sector privado con el financiamiento del crédito.</p>	<p>En el mercado existen entidades financieras que ofrecen créditos, convirtiéndose en un oponente ineludible.</p>
<p>A5</p>	<p>Cambio en las en las políticas de estado que afecten a la institución.</p>	<p>Cambios impuestos por el estado como la cancelación de conceder créditos.</p>

Fuente: Investigación

Elaborado por: Autor de Tesis

PERFIL ESTRATÉGICO EXTERNO

Tabla 13: Perfil Estratégico Externo

ASPECTOS EXTERNOS		CLASIFICACIÓN DE IMPACTO				
		AMENAZAS		NORMAL	OPORTUNIDADES	
		GRAN AMENAZA	AMENAZA	EQUILIBRIO	OPORTUNIDAD	GRAN OPORTUNIDAD
		1	2	3	4	5
O1	Demanda de crédito educativo y becas.					●
O2	Confianza de clientes hacia el IECE.					●
O3	Adquisición de nuevas tecnologías				●	
O4	La educación es objetivo estratégico dentro del Plan Nacional de Desarrollo.					●
O5	Cooperación internacional – APICE					●
A1	Los beneficiarios del crédito no tendrían acceso al mercado laboral, lo que incide en la capacidad de pago del crédito.	●				
A2	La crisis mundial se ve reflejada en una disminución de la oferta de becas internacionales.		●			
A3	Recortes del presupuesto del estado.		●			
A4	Creciente competencia del sector privado con el financiamiento del crédito.	●				
A5	Cambio en las políticas del estado que afecten a la institución.	●				
TOTAL		10				
PORCENTAJE		3	2		1	4
100%		30,00%	20,00%	0%	10,00%	40,00%

Fuente: Investigación

Elaborado por: Autor de Tesis

MATRIZ DE MEDIOS EXTERNO

1= Amenaza Importante.

2= Amenaza Menor.

3= Equilibrio.

4= Oportunidad Menor.

5= Oportunidad Importante.

PONDERACIÓN PERFIL ESTRATÉGICO EXTERNO

Tabla 14: Ponderación Perfil Estratégico Externo

Nº	FACTORES EXTERNOS CLAVES	PONDERACIÓN	CLASIFICACIÓN	RESULTADO PONDERADO
OPORTUNIDADES				
1	Demanda de crédito educativo y becas.	0,10	5	0,50
2	Confianza de clientes hacia el IECE.	0,10	5	0,50
3	Adquisición de nuevas tecnologías	0,10	4	0,40
4	La educación es objetivo estratégico dentro del Plan Nacional de Desarrollo.	0,10	5	0,50
5	Cooperación internacional – APICE	0,10	5	0,50
AMENAZAS				
6	Los beneficiarios del crédito no tendrían acceso al mercado laboral, lo que incide en la capacidad de pago del crédito.	0,10	1	0,10
7	La crisis mundial se ve reflejada en una disminución de la oferta de becas internacionales.	0,10	2	0,20
8	Recortes del presupuesto del estado.	0,10	2	0,20
9	Creciente competencia del sector privado con el financiamiento del crédito.	0,10	1	0,10
10	Cambio en las políticas del estado que afecten a la institución.	0,10	1	0,10
TOTAL		1	31	3,10

Fuente: Investigación

Elaborado por: Autor de Tesis

Análisis:

El resultado de 3.10 obtenido en el análisis nos permite observar que el Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba, se encuentra en equilibrio; las autoridades deben promocionar los servicios que ofrece la entidad y de esta forma obtener nuevos clientes, debido a que la educación es un objetivo estratégico en el plan nacional de desarrollo y que todas las personas buscan su superación profesional, también debe contar con un software adecuado que mejore la calidad en la prestación del servicio, las autoridades y funcionarios deben en lo posible neutralizar las amenazas existentes para no tener un impacto perjudicial en la institución.

CAPÍTULO IV

4. AUDITORÍA INFORMÁTICA AL INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS (IECE) REGIONAL 3 RIOBAMBA

4.1 GENERALIDADES

4.1.1 ALCANCE

La Auditoría Informática aplicada al Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba, con énfasis a la unidad de TICs, comprende el estudio y análisis de las Tecnologías de Información y Comunicación TICs y la gestión informática.

4.1.2 OBJETIVO

El Objetivo General es realizar una Auditoría Informática al Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba, evaluando la utilización y aprovechamiento de las TICs y la gestión informática.

4.1.3 BASE LEGAL

Para el desarrollo del presente proyecto de tesis tomamos como referencia las Normas de Control Interno referente a Tecnologías de la Información y Comunicación emitidas por la Contraloría General del Estado.

4.1.4 METODOLOGÍA

Para la realización de la Auditoría Informática se va tomar como base las Normas de Control Interno emitidas por la Contraloría General del Estado, del sub grupo 400 referente a las Normas de Tecnologías de Información y Comunicación.

La Contraloría General del Estado también emite una guía metodológica para la realización de auditorías a las instituciones públicas y basándose en esta guía metodológica la auditoría se va realizar en las siguientes etapas:

- Planeación
- Ejecución
- Comunicación de resultados

a) **PLANEACIÓN:** En la planeación de una Auditoría Informática se deben cumplir varias tareas: 1) Conocimiento de la entidad a través del relevamiento de información, 2) Evaluación de control interno y 3) Diseño de un programa de auditoría.

Los objetivos específicos de la Auditoría Informática identificarán los temas prioritarios a evaluar; estarán en relación con el criterio de eficiencia en el manejo de los recursos informáticos, y de efectividad, legalidad e impacto en el logro de metas y objetivos. La fase de planificación en la Auditoría Informática, parte del conocimiento preliminar hasta la formulación del programa de auditoría.

A continuación se presenta las actividades a realizar en la etapa de planeación:

ACTIVIDADES A REALIZAR EN LA ETAPA DE PLANEACIÓN	
1. Conocimiento preliminar de la unidad de TICs.	<p>Las actividades a realizar son:</p> <ul style="list-style-type: none"> a) Realizar una entrevista al encargado de la unidad de TICs; esta entrevista se lo realizará con preguntas abiertas, de sondeo y cerradas; al momento de realizar la entrevista se debe estar bien preparado, cumplir con los tiempos planeados, darle tranquilidad al auditado y no hacer juicios de valor. b) Solicitar el organigrama de la institución para verificar si la unidad de TICs se encuentra en un nivel que permita brindar asesoría y apoyo a la alta dirección. c) Verificar si dispone de un manual de funciones para el personal de la unidad de TICs. d) Verificar si dispone de un manual de políticas y procedimientos para unidad TICs. <p>Al obtener esta información nos permitirá conocer su historia, su estructura organizacional y si la unidad de TICs dispone de políticas claves para su correcto funcionamiento.</p>

<p>2. Evaluación del sistema de control interno TICs.</p>	<p>La evaluación del sistema de control interno de las TICs, permitirá acumular información sobre el funcionamiento de los controles existentes e identificar los asuntos que requieran profundizarse en la fase de ejecución del examen.</p> <p>Las actividades a realizar son:</p> <p>a) Aplicar cuestionarios de control interno; estos cuestionarios serán elaborados basados en las Normas de Control Interno emitidas por la Contraloría General del Estado, del sub grupo 400 referente a las Normas de Tecnologías de Información estas son:</p> <ul style="list-style-type: none"> • Organización informática. • Segregación de funciones. • Plan informático estratégico de tecnología. • Políticas y procedimientos. • Modelo de información organizacional. • Administración de proyectos tecnológicos. • Desarrollo y adquisición de software aplicativo. • Adquisiciones de infraestructura tecnológica. • Mantenimiento y control de la infraestructura tecnológica. • Seguridad de tecnología de la información. • Plan de contingencias. • Administración de soporte de tecnología de información. • Monitoreo y evaluación de los procesos y servicios. • Sitio web, servicios de internet e intranet. • Capacitación informática. • Comité informático. • Firmas electrónicas. <p>Norma 500 Información y Comunicación:</p> <ul style="list-style-type: none"> • Controles sobre sistemas de información. • Canales de comunicación abiertos. <p>El cuestionario de control interno contendrá lo siguiente:</p> <ul style="list-style-type: none"> • Nombre de la entidad. • Área Auditada.
--	---

	<ul style="list-style-type: none"> • Componente. • Motivo del Examen. • Preguntas. • Respuestas. • Comentario. • Total. (Ver anexo 2) <p>b) Definir la ponderación de cada una de las preguntas; la ponderación de las preguntas tendrán una puntuación de 10 mientras que la calificación varia del 1 al 10 según el criterio del auditor observando, verificando y constatando cómo se encuentran realizando las actividades de las preguntas que sean efectuado al auditado, al final se realizará la suma de la ponderación y calificación.</p> <p>La matriz de ponderación contendrá lo siguiente</p> <ul style="list-style-type: none"> • Nombre de la entidad. • Preguntas. • Ponderación. • Calificación. • Total. (Ver anexo 3) <p>c) Determinación del nivel de confianza y riesgo; para la determinación del nivel de riesgo se aplicara la siguiente fórmula:</p> $CONFIANZA PONDERADA = \frac{Calificación\ Total}{Ponderación\ Total} * 100$ <p>Se aplicará también una tabla de riesgo y confianza que contendrá lo siguiente:</p> <ul style="list-style-type: none"> • Rango • Riesgo • Confianza (ver anexo 4) <p>En base al resultado obtenido se realizará un análisis de las actividades evaluadas.</p>
<p>3. Determinación de áreas críticas.</p>	<p>Sobre la base de los resultados de la evaluación del sistema de control interno de las TICs, se determinarán las áreas críticas, que serán las que presenten deficiencias de control por la ausencia de</p>

	<p>controles o porque los existentes no funcionan o son innecesarios; seleccionando las de mayor importancia relativa.</p> <p>Se elaborará una matriz que muestre el impacto que las deficiencias de control causan en la unidad de TICs. Esta matriz contendrá lo siguiente:</p> <ul style="list-style-type: none"> • Detalle. • Nivel de riesgo. • Causa. • Impacto. • Acciones recomendadas. • Norma relacionada. (Ver anexo 5)
<p>4. Elaboración de los programas de auditoría.</p>	<p>Los programas para la Auditoría Informática describen específicamente como se deben llevar a cabo las actividades durante la ejecución del examen, contienen una relación ordenada de forma secuencial y lógica de los diferentes procedimientos a desarrollarse en relación a los objetivos propuestos, en cada programa, procesos o actividades a examinarse.</p> <p>Los programas serán elaborados por el auditor encargado del análisis, considerando lo siguiente:</p> <ul style="list-style-type: none"> • Objetivos • Procedimientos <p>El programa de auditoría contendrá lo siguiente:</p> <ul style="list-style-type: none"> • Nombre de la entidad auditada. • Área auditada. • Tipo de auditoría. • Fase. • Objetivo. • Procedimientos. (Ver Anexo 6) <p>El mismo que se elaborará de acuerdo a las necesidades a evaluarse en cada etapa de la metodología, permitiendo llevar un control adecuado de los procedimientos a auditarse. Los procedimientos se formularán con cierta flexibilidad que permita modificaciones cuando se necesite profundizar en los hallazgos encontrados y</p>

	generar recomendaciones aplicables, oportunas y pertinentes que ayuden a la entidad auditada a corregir las deficiencias.
--	---

b) EJECUCIÓN: En esta etapa, se ejecuta el trabajo de auditoría, con el desarrollo de los programas y con la obtención de la evidencia suficiente, relevante y competente, basada en criterios de auditoría y procedimientos definidos en cada programa; a través de los que se conocerán aspectos relacionados con la utilización y aprovechamiento de TICs en la entidad bajo examen.

A continuación se presenta las actividades a realizar en la etapa de ejecución:

ACTIVIDADES A REALIZAR EN LA ETAPA DE EJECUCIÓN	
1. Obtención de evidencia.	<p>Las evidencias pueden ser: físicas, documentales, testimoniales y analíticas, y deberán ser evaluadas para el desarrollo de los hallazgos, verificando que cumplan con las siguientes condiciones:</p> <ul style="list-style-type: none"> • Suficiencia del trabajo realizado; es decir, recopilación de hechos reales, adecuados y convincentes. • Confiabilidad de los antecedentes obtenidos; los antecedentes deberán ser válidos y confiables, es decir que reflejen la situación real de la unidad examinada. <p>Factores a considerar:</p> <ul style="list-style-type: none"> • La evaluación de la naturaleza y nivel del riesgo de la unidad de TICs. • Naturaleza de los sistemas de control interno y la evaluación del riesgo de control. • Importancia relativa del componente a examinar. • Fuente y confiabilidad de información disponible.
2. Aplicación de indicadores.	<p>Los indicadores nos permitirán medir de forma cuantitativa y cualitativa, el grado de cumplimiento de un sistema, proyecto, programa, componente, proceso, actividad o de la ejecución de las operaciones, en términos de eficiencia, economía, efectividad e impacto.</p> <p>Los indicadores se presentarán en una matriz denominada ficha técnica, que contiene la siguiente información:</p>

	<ul style="list-style-type: none"> • Nombre del indicador. • Factores críticos de éxito. • Fórmula de cálculo del índice. • Frecuencia. • Valores. • Porcentaje. • Interpretación. (Ver Anexo 7)
3. Criterios de auditoría.	<p>Los criterios a utilizarse en la Auditoría Informática son:</p> <ul style="list-style-type: none"> • Disponibilidad de un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control en la entidad. • Funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información. • Los sistemas informáticos son evaluados periódicamente, con el fin de detectar fallas que puedan afectar a las operaciones. • Cumplimiento de la Normativa en este ámbito. • Revisión de la eficaz gestión de los recursos informáticos • La medición del desempeño de la unidad de TICs es apropiada. • El desempeño debe ser adecuado, en comparación con el estándar. • El nivel actual de rendimiento debe ser aceptable, en comparación con la base establecida.
4. Papeles de trabajo.	<p>Los papeles de trabajo constituyen los programas escritos con la indicación de su cumplimiento y la evidencia reunida por el auditor en el desarrollo de su tarea; será el vínculo entre el trabajo de planeamiento, de ejecución y del informe de auditoría, por tanto contendrán la evidencia necesaria para fundamentar los hallazgos, opiniones, conclusiones y recomendaciones que se presenten en el informe.</p>

c) **COMUNICACIÓN DE RESULTADOS:** En esta etapa se dará a conocer los hallazgos encontrados durante la evaluación en la utilización y aprovechamiento de las tecnologías de información a través del informe final de auditoría.

A continuación se presenta las actividades a realizar en la etapa de comunicación de resultados:

ACTIVIDADES A REALIZAR EN LA ETAPA DE COMUNICACIÓN DE RESULTADOS	
1. Determinación de Hallazgos.	<p>Se presentara de forma objetiva los hechos observados o encontrados durante la ejecución de la auditoría.</p> <p>Un hallazgo debe tener ciertos requisitos:</p> <ul style="list-style-type: none"> • Importancia relativa que merezca su comunicación. • Debe basarse en hechos y evidencias precisas que figuran en los papeles de trabajo. • Convincente a una persona que no ha participado en la auditoria. <p>Se lo realizara en base a los atributos del hallazgo:</p> <p>1. Condición: La realidad encontrada</p> <p>2. Criterio: Cómo debe ser (la norma, la ley, el reglamento, lo que debe ser).</p> <p>3. Causa: Qué originó la diferencia encontrada.</p> <p>4. Efecto: Qué efectos puede ocasionar la diferencia encontrada.</p> <p>Se establecerán también las conclusiones y recomendaciones para mitigar las deficiencias encontradas.</p>
2. Elaboración de carta de presentación.	<p>A través de esta carta se informa al gerente, que ya se finalizó la auditoría, se indicará el período auditado, bajo que normas se efectuó y se indicará que se obtuvieron resultados de la auditoría realizada.</p>
3. Elaboración del informe final de auditoría.	<p>En el informe de auditoría se comunicará:</p> <ul style="list-style-type: none"> • El motivo del examen • Los objetivos de la auditoria. • Las normas utilizadas. • El alcance. • Resultados de la auditoría.

	El informe debe ser objetivo, claro, conciso, constructivo y oportuno.
4. Elabore el acta de convocatoria.	Según lo dispuesto en los artículos 90 de la Ley Orgánica de la Contraloría General del Estado y 23 de su reglamento se convocara al gerente y personal auditado a la reunión que se realizará para comunicar los resultados obtenidos. En el acta se indicara el lugar y la fecha que se va a llevar acabo la reunión.
5. Realización de la convocatoria.	Con la presencia de los funcionarios auditados se procederá a dar a conocer los resultados obtenidos en la auditoría informática efectuada.

4.1.5 HOJA DE MARCAS

MARCAS	SIGNIFICADO
✓	Verificado mediante inspección física
@	Analizado
↔	Comparado
⇒	Determinación de hallazgo
∝	Cotejado con inventarios
⊗	Incluir en informe
≠	Cotejado con documentos
S	Documentación sustentatoria
^	Transacción rastreada
Σ	Comprobado sumas
C	Circularizado
℄	Confirmado
N	No autorizado

4.1.6 ABREVIATURAS

AF	=	Análisis FODA
PA	=	Programa de Auditoría
FP	=	Fase Preliminar
FE	=	Fase de Ejecución
HA	=	Hoja de Hallazgos
CR	=	Fase de Comunicación de Resultados
CGE	=	Contraloría General de Estado

ETAPAS DE LA AUDITORÍA INFORMÁTICA

PRIMERA ETAPA: PLANEACIÓN

PROGRAMA DE AUDITORÍA

Entidad: IECE Regional 3 Riobamba
Área: TIC del IECE
Tipo de Auditoría: Auditoría Informática.
Fase: Planeación

Objetivo: Adquirir el conocimiento necesario de la historia, estructura organizacional y actividades que realiza la entidad para iniciar con el desarrollo de la Auditoría Informática.

Nº	DESCRIPCIÓN	REF. PT.	ELABORADO POR:	FECHA
PROCEDIMIENTOS				
1	Realice una carta compromiso indicando que se iniciara con el desarrollo de la auditoría, a fin de que se brinde las facilidades para el desarrollo de la misma.	FP1	AMOY	17/07/13
2	Realice una entrevista al encargado de la unidad de tecnología de información para obtener información general de esta unidad.	FP2	AMOY	19/07/13
3	Solicite el organigrama de la institución a fin de determinar si la unidad de TICs cumple la función de asesoría y apoyo dentro del mismo.	FP3	AMOY	19/07/13
4	Solicite manual de funciones del personal de la unidad.	FP4	AMOY	22/07/13
5	Solicite manual de políticas y procedimientos de la unidad.	FP5	AMOY	22/07/13
6	Evaluación del Sistema de control interno TICs	FP6	AMOY	23/07/13
7	Determinación de áreas Críticas	FP7	AMOY	26/07/13

Riobamba, 15 de julio del 2013

Economista

Yesenia Díaz

GERENTE DEL IECE REGIONAL 3 RIOBAMBA

Presente

De mi consideración:

En atención al pedido que se realizó para la ejecución de la Auditoría Informática al Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba, correspondiente al período del 01 de Enero al 31 de Diciembre del 2012.

El Señor Alex Mauricio Obando Yumisaca, realizará la Auditoría Informática de acuerdo a las normas de control interno emitidas por la Contraloría General del Estado en lo referente a tecnologías de información y comunicación, con el fin de obtener una opinión del aprovechamiento y utilización de las TICs, el mismo que se llevara a cabo a través de aplicación de encuestas, entrevistas, inspecciones físicas, pruebas técnicas y de campo, revisión de documentos y análisis de los mismos con el fin de obtener evidencia que sustente mi opinión.

Al mismo tiempo de la manera más comedida solicito la completa colaboración y facilidades por parte del personal que labora en la entidad en especial al personal de la unidad de TICs, para acceder a la respectiva documentación, para evaluar los parámetros establecidos y el cumplimiento de los objetivos y la optimización y buen uso de los recursos.

Por la atención a la presente, anticipo mis sinceros agradecimientos.

Atentamente,

Sr. Alex Obando

REALIZADO POR: AMOY	FECHA: 17-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

ENTREVISTA: Encargado de la unidad de TICs del IECE Regional 3

FECHA: 18/07/2013

1. ¿Cuál es la fecha de creación de la unidad de TICs en el IECE Regional 3 Riobamba?

La unidad de TICs en el Instituto Ecuatoriano de Crédito Educativo y Becas IECE Regional 3 Riobamba, se creó en septiembre de 2008 bajo la administración del Dr. Lenin Broz Tito Ruilova gerente de la institución y a cargo de la Unidad de TIC hasta hoy el Ing. Marcelo Monar.

2. ¿Con qué finalidad se creó la unidad de TICs en la entidad?

La unidad de TICs se creó con la finalidad de atender las necesidades y requerimientos que tienen que ver con el desempeño del parque informático en la Regional 3 Riobamba.

3. ¿Quiénes son los responsables, que funciones y actividades cumplen el personal operativo de esta unidad?

Responsable: Ing. Marcelo Monar

Las funciones y actividades que realiza son:

- Brindar soporte a los sistemas informáticos, equipos informáticos.
- Realizar un seguimiento del funcionamiento del parque informático.
- Monitorear los enlaces internos solventar los requerimientos existentes.
- Mantener en buen estado el cableado estructurado en la institución.
- Realizar reportes periódicos sobre el plan de acción y contingencia respecto a la unidad de TICs.
- Responsable de los procedimientos del INCOP.

REALIZADO POR: AMOY	FECHA: 19-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

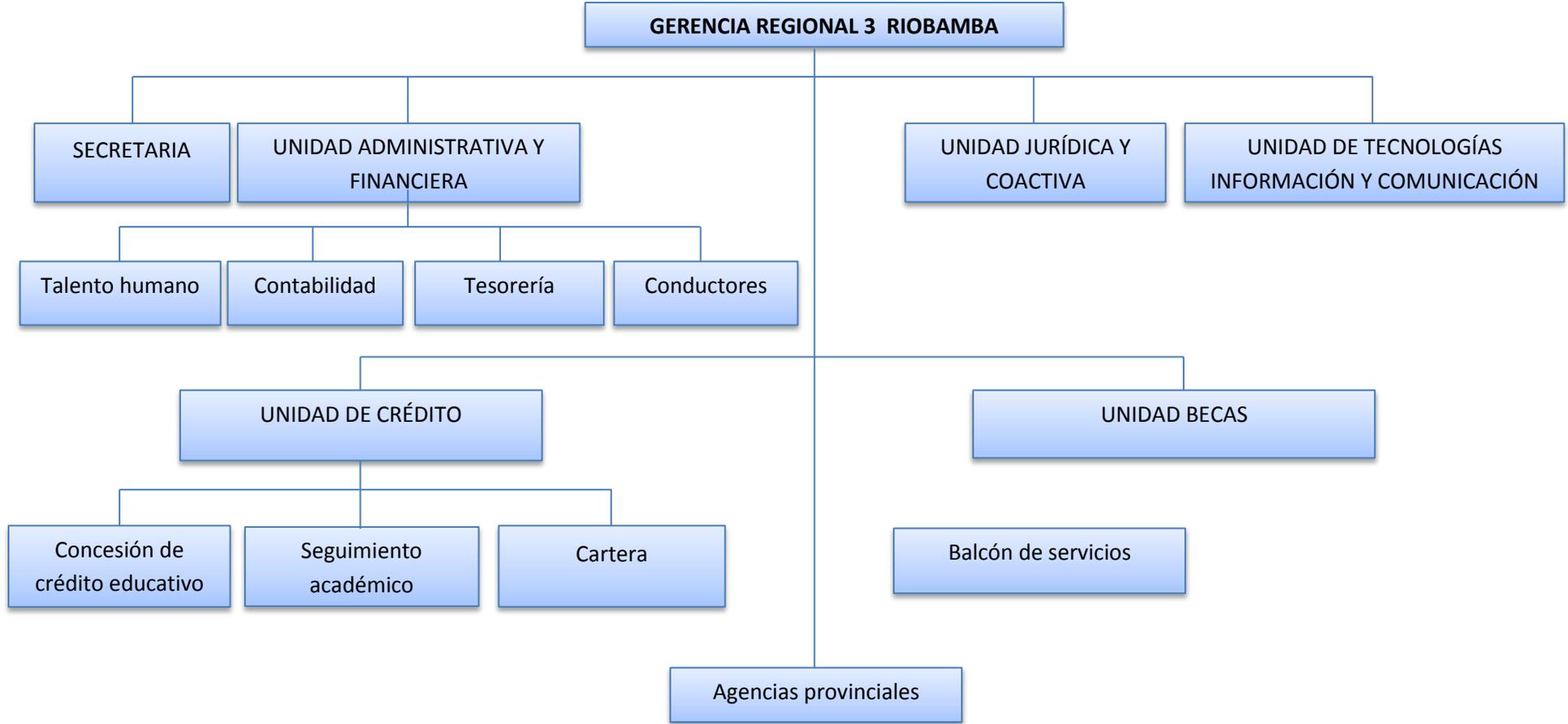
4. ¿Se ha efectuado alguna auditoría informática en la entidad?

No se ha realizado Auditorías Informáticas por lo que se ha visto de manera oportuna que se proceda a la petición del estudiante de Contabilidad y Auditoría de la Escuela Superior Politécnica de Chimborazo con la aplicación de una auditoría informática para determinar el aprovechamiento y utilización de las TICs en la entidad.

REALIZADO POR: AMOY	FECHA: 19-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

Organigrama IECE Regional 3 Riobamba

Figura 4: Organigrama Institucional



Fuente: Reglamento Orgánico de Gestión por Procesos del Instituto Ecuatoriano de Crédito Educativo y Becas
Elaborado por: El Autor de tesis

REALIZADO POR: AMOY	FECHA: 19-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

La unidad de TICs consta en el organigrama del Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba y su encargado el Ing. Marcelo Monar manifiesta que la unidad de TICs se encuentra en un nivel que permite brindar asesoría y apoyo a la alta dirección y a las demás unidades usuarias y según el orgánico funcional de la institución refleja esta situación.

REALIZADO POR: AMOY	FECHA: 19-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

Funciones del personal de la unidad de TICs.

La unidad de TICs dispone de las siguientes funciones para el personal:

- Formateo de computadores PC y portátiles de la regional y agencias.
- Elaborar el inventario del equipo informático de la regional y sus agencias.
- Brindar soporte técnico a usuarios en los aplicativos informáticos.
- Brindar soporte técnico al parque informático en la regional y agencias.
- Actualizar versiones de los sistemas institucionales SIGEN, SIB, BECAS SENESCYT.
- Monitoreo del correcto funcionamiento de los enlaces de datos externos.
- Administración de servidores.
- Administración y configuración de servidor Linux, Samba.

Ver Anexo 8

REALIZADO POR: AMOY	FECHA: 22-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS

Entre las políticas que dispone la unidad de TICs están las siguientes:

- Políticas de uso de la red.
- Políticas de uso de internet.
- Políticas de correo electrónico.
- Políticas de seguridad de servicios.
- Políticas de DW de antivirus.
- Políticas de Seguridad de usuarios y contraseñas.
- Políticas de creación de usuario de aplicaciones institucionales.
- Políticas de contraseñas de usuario Quipux
- Políticas de uso de información y respaldos (Backup).
- Políticas para dueños de la información.
- Políticas de uso del sistema de gestión soporte Aranda Service DESk.
- Políticas de los dispositivos periféricos.
- Políticas de uso del computador personal.

Ver anexo 9

REALIZADO POR: AMOY	FECHA: 22-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

DETERMINACIÓN DE ÁREAS CRÍTICAS

DETALLE	NIVEL DE RIESGO	CAUSA	IMPACTO	ACCIONES RECOMENDADAS	NORMA RELACIONADA
La unidad de TICs no dispone de la facilidad de tomar decisiones y generar cambios de mejora tecnológica.	Bajo	Depende de la coordinación con la matriz.	No genera cambios de mejora en la unidad.	Que el encargado de la unidad comunique su inconformidad a gerencia y conseguir su desconcentración de la matriz.	410-01 Organización Informática.
La unidad de TICs no cuenta con el personal suficiente para realizar sus actividades.	Bajo	Falta de un estudio para analizar si el personal existente es el suficiente para cumplir con sus actividades.	Sobrecarga laboral al único funcionario existente en la unidad de TICs.	Verificar si es necesario contratar personal adicional.	410-02 Segregación de funciones.
La unidad de tecnología de información no promueve ni establece convenios con otras organizaciones o terceros a fin de promover y viabilizar el intercambio de información interinstitucional.	Bajo	Esta es responsabilidad de la unidad de comunicación en coordinación con la gerencia regional y la gerencia general.	Desconocimiento por parte de la unidad de TICs de los convenios con otras organizaciones o terceros.	Involucrarse en este tema debido a que es competencia de la unidad de TICs según lo dispuesto por las normas de control interno emitidas por la CGE.	410-04 Políticas y procedimientos.
La unidad de tecnología de información no cuenta con un modelo de información organizacional.	Alto	Esto se lo realiza en la matriz y lo ejecuta la unidad de comunicación.	Afecta a la regional debido a que no dispone de un modelo de información organizacional.	Que el encargado de la unidad de TICs de la regional defina un modelo de información organizacional en la regional a fin de que se facilite su uso y compartición.	410-05 Modelo de información organizacional.
Desconocimiento sobre la adquisición de software o soluciones tecnológicas si este se realiza sobre la base del portafolio de proyectos y servicios priorizados en los planes estratégico y operativo del IECE.	Medio	La regional 3 Riobamba no realiza este proceso, lo realiza la matriz.	La unidad de TICs de la regional no puede regular los procesos de desarrollo y adquisición de software aplicativo.	Crear aplicativos intermedios para poder tener acceso a información de la unidad de TICs de la matriz.	410-07 Desarrollo y adquisición de software aplicativo.

REALIZADO POR: AMOY	FECHA: 26-072013
REVISADO POR: BNCO	FECHA: 17-08-2013

Falta reforzar la evaluación de los riesgos, vulnerabilidades y los requerimientos de seguridad.	Bajo	No se toma en cuenta la necesidad de evaluar los riesgos, vulnerabilidades y los requerimientos de seguridad para la unidad de TICs de la regional.	Se pone en riesgo el parque informático al no considerar los riesgos a los que están expuestos.	Evaluar los riesgos, vulnerabilidades y los requerimientos de seguridad.	410-09 Mantenimiento y control de la infraestructura tecnológica.
La unidad de TICs no cuenta con una ubicación adecuada.	Medio	Se acopla de acuerdo al espacio disponible en la entidad.	No cuenta con una ubicación adecuada, ni seguridades necesarias para ejecutar sus actividades.	Incorporar seguridades necesarias para hacer de la unidad de TICs un lugar más seguro.	410- 10 Seguridad de tecnología de información.
El plan de contingencias de la unidad de TICs no es el adecuado.	Alto	No se consideran aspectos necesarios para que el plan de contingencia sea el adecuado.	No permite reaccionar inmediatamente ante cualquier eventualidad.	Reestructurar el plan de contingencias, indicando las actividades a realizar en caso de alguna eventualidad y sociabilizar con los responsables de su ejecución.	410- 11 Plan de contingencias.
No se define el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad.	Medio	No se tiene definido el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad.	No se monitorea la contribución y el impacto de la tecnología de información en la entidad.	Establecer un marco de trabajo, el cual disponga de los procesos a seguir para monitorear la contribución y el impacto de la tecnología de información.	410-13 Monitoreo y evaluación de los procesos y servicios.
Desconocimiento de aspectos en la adquisición y mantenimiento de la firma electrónica.	Medio	Dependencia de la matriz.	No permite conocer al funcionario aspectos acerca de la adquisición y mantenimiento de la firma electrónica.	Crear aplicativos intermedios para poder tener acceso a información de la unidad de TICs de la matriz.	410-17 Firmas Electrónicas.

REALIZADO POR: AMOY	FECHA: 26-072013
REVISADO POR: BNCO	FECHA: 17-08-2013

SEGUNDA ETAPA: EJECUCIÓN
PROGRAMA DE AUDITORÍA

Entidad: IECE Regional 3 Riobamba
Área: TIC del IECE
Tipo de Auditoría: Auditoría Informática.
Fase: Ejecución

Objetivo: Obtener evidencia suficiente, competente, relevante y pertinente que permita conocer aspectos relacionados con la utilización y aprovechamiento de TICs en la entidad bajo examen.

Nº	DESCRIPCIÓN	REF. PT.	ELABORADO POR:	FECHA	OBSERVACIONES
PROCEDIMIENTOS					
1	Revise la planificación de la unidad bajo examen y determine su relación con los objetivos de la entidad y del Plan Nacional de Desarrollo	FE 1	AMOY	02/08/13	
2	Verifique si los procesos o programas a cargo de la unidad auditada, se están ejecutando razonablemente.	FE 2	AMOY	04/08/13	
3	Verificar debilidades encontradas en la norma 410-01 Organización Informática (dispone de la facilidad de tomar decisiones y generar cambios de mejora.)	FE 3	AMOY	06/08/13	Dependencia de la matriz
4	Verificar debilidades encontradas en la norma 410-02 segregación de funciones (la unidad TICs cuenta con el personal suficiente para realizar sus actividades.)	FE 4	AMOY	09/08/13	
5	Solicite el modelo de información organizacional.	FE 5	AMOY	09/08/13	No existe
6	Solicite los procesos para el desarrollo y adquisición de software aplicativo.	FE 6	AMOY	09/08/13	No dispone
7	Solicite contratos de compra o renta de software.	FE 7	AMOY	09/08/13	No dispone
8	Solicite planificación de mantenimiento de equipos.	FE 8	AMOY	09/08/13	

9	Realice verificación física sobre las medidas de seguridad disponibles en la unidad de TICs.	FE 9	AMOY	13/08/13	
10	Realice verificación física de las condiciones de las unidades de la entidad.	FE 10	AMOY	16/08/13	
11	Realice verificación de políticas de cambio de claves de acceso por parte del personal.	FE 11	AMOY	23/08/13	
12	Solicite el plan de contingencias de la unidad de TICs.	FE 12	AMOY	01/09/13	
13	Solicite el manual de políticas internas de manejo y archivo de información digital.	FE 13	AMOY	01/09/13	
14	Solicite políticas de documentación y eliminación de archivo.	FE 14	AMOY	01/09/13	
15	Solicite cronograma de actividades, metas y objetivos de la unidad de TICs.	FE 15	AMOY	15/09/13	
16	Solicitar inventario de hardware y software.	FE 16	AMOY	22/09/13	
17	Mediante inspección física seleccione al azar y verifique dicha información.	FE 17	AMOY	22/09/13	
18	Aplicación de indicadores.	F 18	AMOY	22/09/13	

PLANIFICACIÓN DE LA UNIDAD Y SU RELACIÓN CON LOS OBJETIVOS DE LA ENTIDAD Y DEL PLAN NACIONAL DE DESARROLLO.

UNIDAD DE TICs	IECE REGIONAL 3	PLAN NACIONAL DE DESARROLLO
OBJETIVOS		
<p>1. Mantener en óptimas condiciones todos los equipos informáticos para el óptimo desempeño de las funciones y operaciones institucionales.</p> <p>2. Garantizar la continuidad del funcionamiento del Hardware, Software y los servicios al máximo rendimiento.</p> <p>3. Mantener operativos todos los enlaces, redes y bases de datos de los sistemas institucionales a fin de mantener la eficiencia y eficacia en los procesos.</p> <p>4. Promover la generación de nuevas aplicaciones de calidad, acordes con las necesidades institucionales, a fin de brindar el mejor servicio a la colectividad con calidad y calidez.</p>	<p>1. Conceder crédito educativo y becas de acuerdo a los criterios de priorización establecidos en la política pública.</p> <p>2. Mejorar continuamente la administración del IECE bajo los principios constitucionales de eficacia, eficiencia, calidez a través de estándares de calidad en los servicios e infraestructura que ofrece la Institución</p> <p>3. Mantener y ampliar la cobertura de los servicios a nivel nacional</p> <p>5. Administrar de manera eficiente los fondos y ofertas de becas provenientes de organismos e instituciones nacionales e internacionales.</p> <p>6. Contar con sistemas integrados acorde a la nueva tecnología, proveer a la institución del parque informático suficiente.</p> <p>7. Ejecutar la política pública para la operativización de la entrega de los servicios y productos institucionales.</p> <p>8. Contar con una estructura orgánica y normativa actualizada.</p> <p>9. Desarrollar y ejecutar un plan anual de contrataciones enmarcado en los objetivos del PNBV y los objetivos institucionales.</p>	<p>1. Auspiciar la igualdad, la cohesión y la integración social y territorial en la diversidad.</p> <p>2. Mejorar las capacidades y potencialidades de la ciudadanía.</p> <p>3. Mejorar la calidad de vida de la población.</p> <p>4. Garantizar el trabajo estable, justo y digno, en su diversidad de formas.</p> <p>5. Garantizar la vigencia de los derechos y la justicia.</p> <p>6. Garantizar el acceso a la participación pública y política.</p> <p>7. Establecer un sistema económico social, solidario y sostenible.</p> <p>8. Construir un Estado Democrático para el Buen Vivir.</p>

Los objetivos de la unidad de TICs tienen relación con los objetivos de la entidad y éste a su vez con los objetivos del plan nacional de desarrollo, el IECE busca mecanismos legales y técnicos que permitan financiar la formación del talento humano de todos los ecuatorianos, de preferencia en los de escasos recursos económicos, a través del crédito educativo reembolsable y no reembolsable, becas, ayudas económicas y otros mecanismos de integración y equidad social.

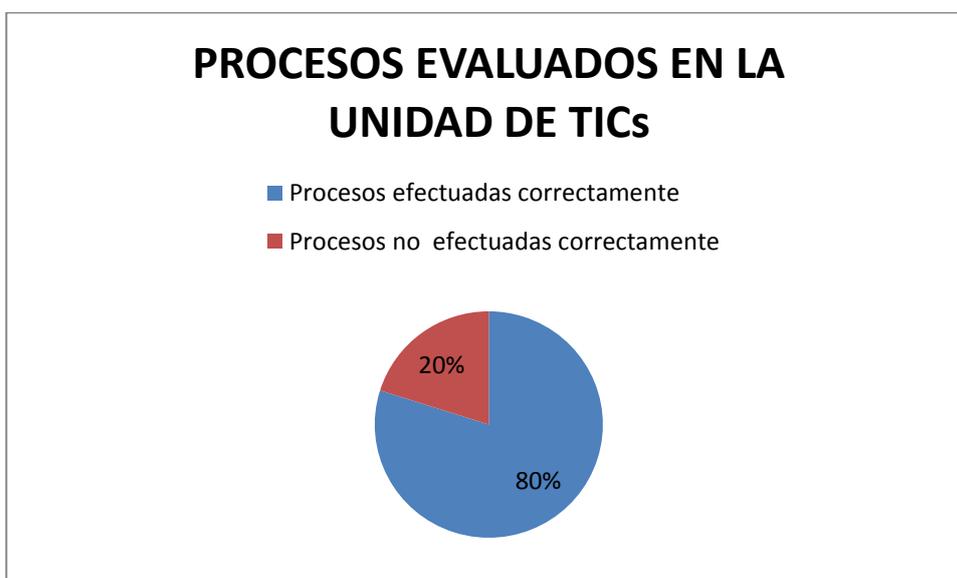
REALIZADO POR: AMOY	FECHA: 02-08-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

VERIFICACIÓN DE PROCESOS EJECUTADOS EN LA UNIDAD DE TICs

En base a la evaluación de control interno efectuada a la unidad de TICs, se obtiene los siguientes resultados:

Procesos evaluados	19
Actividades evaluadas	154
Actividades efectuadas correctamente	123
Actividades no efectuadas correctamente	31

En el siguiente grafico se puede observar el resultado en porcentaje:



Como se puede observar en el grafico los procesos efectuados correctamente en la unidad de TICs es el 80%, sin embargo existen un 20% restante el cual se debe mejorar.

REALIZADO POR: AMOY	FECHA: 04-08-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

SEGREGACIÓN DE FUNCIONES: La unidad de TICs cuenta con un solo funcionario para realizar las actividades para verificar si se requiere contratar un funcionario adicional se empleó los siguientes indicadores:

NOMBRE DEL INDICADOR	FACTORES CRÍTICOS DE ÉXITO	FORMULA DE CALCULO	FRECUENCIA	VALORES	%	INTERPRETACIÓN
Porcentaje de horas planeadas en órdenes de trabajo totales en la unidad de TICs.	Empleo adecuado de las horas hombre disponible.	$\frac{\text{Hrs planeadas en órdenes de trabajo totales}}{\text{Hrs hombre disponibles}}$	Mensual	$\frac{41,45}{40} \times 100$	103,63 %	Se puede observar que en la unidad de TICs se sobre pasa las horas hombre disponible, por lo que se debe considerar contratar personal adicional para la unidad.
Porcentaje de actividades ejecutadas en la unidad de TICs.	Cumplimiento oportuno y adecuado de las actividades planificadas en la unidad de TICs.	$\frac{\text{Total actividades ejecutadas}}{\text{Total actividades planificadas}}$	Mensual	$\frac{6}{8} \times 100$	75%	Se puede observar que en la unidad de TICs no existe un cumplimiento adecuado de las actividades planificadas.

REALIZADO POR: AMOY	FECHA: 09-08-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

PLAN DE CONTINGENCIAS DE LA UNIDAD DE TICs
ASPECTOS POSITIVOS DEL CONTENIDO DEL PLAN DE CONTINGENCIAS
La unidad de TICs de la regional 3 Riobamba dispone de un plan de contingencias, el cual permite recuperar la operación de los sistemas en un nivel aceptable.
La aplicación del plan de contingencias permite salvaguardar la integridad y seguridad de la información.
El plan de contingencias cuenta con un plan de continuidad de las operaciones.
El plan de contingencias cuenta con procedimientos de control de cambios.
ASPECTOS NEGATIVOS DEL CONTENIDO DEL PLAN DE CONTINGENCIAS
El plan de contingencias no dispone de un plan de respuesta a los riesgos.
No cuenta con un plan de recuperación de desastres.
No se ha designado un comité con nombres y roles específicos para ejecutar las funciones de contingencia en caso de suscitarse una emergencia.
El plan de contingencias aprobado, no es difundido entre el personal responsable de su ejecución.
El plan de contingencias no es sometido a pruebas, entrenamientos y evaluaciones periódicas.

REALIZADO POR: AMOY	FECHA: 01-09-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

MANUAL DE POLÍTICAS INTERNAS DE MANEJO Y ARCHIVO DE INFORMACIÓN DIGITAL
La institución dispone de un manual de políticas internas de manejo y archivo de información digital; por lo que todos los documentos generados, recibidos y digitalizados en la institución son de exclusividad y propiedad del IECE y por ninguna razón deberán ser utilizados para conformar archivos privados de los funcionarios que laboran en la institución.
El responsable de su cumplimiento será el gerente de la regional.
SUS PROCESOS HABILITADORES SON:
Documentación habilitada.
Proceso gestorador.
Proceso de escaneado.
Proceso de digitalización.
Proceso de control de calidad.
Prohibición de acceso a archivos reservados.
Prohibición y sanciones generales.

Ver Anexo 10

REALIZADO POR: AMOY	FECHA: 01-09-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

POLÍTICAS DE DOCUMENTACIÓN Y ELIMINACIÓN DE ARCHIVO

La institución dispone de políticas de documentación y eliminación de archivo; su propósito es normar el proceso de selección, evaluación, conservación y eliminación de documentos que han perdido su valor permanente.

ENVÍO DE DOCUMENTOS.- Todas las unidades remitirán al Archivo Pasivo del IECE, en caja de cartón, los documentos que hayan cumplido un tiempo de permanencia de tres (3) años en la unidad, contados a partir de la fecha de emisión; mediante acta entrega – recepción, por duplicado.

INVENTARIO DE ELIMINACIÓN DE DOCUMENTOS.- Dentro de los 15 primeros días de enero de cada año, la Secretaría General identificará la documentación a eliminarse, conforme a los plazos de vigencia y conservación.

CONFORMACIÓN DE LA COMISIÓN.- Se conforma la Comisión de Evaluación y Eliminación de Documentos, que estará integrada por los siguientes miembros:

- a) El Secretario General o su delegado, quien la presidirá;
- b) El Gerente de Asesoría Jurídica o su delegado; y,
- e) El Gerente del Proceso responsable de la documentación a darse de baja, un delegado de Auditoría Interna.

PLAZOS DE VIGENCIA Y CONSERVACIÓN.-

Tres meses.- Salvoconductos, control de ingresos de personas particulares y circulares emitidas por la Gerencia General.

Tres años.- Oficios y memorandos de carácter administrativo, revistas informativos, registros oficiales, presupuestos, planes operativos, planes de marketing, notas de pedido, control de vehículos de la Entidad, permisos particulares, acciones de personal por vacaciones, licencias, comisiones de servicio y sanciones administrativas que no tengan incidencia financiera, registros de asistencia, expedientes de exfuncionarios y empleados y otros similares;

Cinco años.- Resoluciones del Directorio, estadísticas, convenios y respaldos de información por medios magnéticos.

REALIZADO POR: AMOY	FECHA: 01-09-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

Seis años.- Estados financieros, documentación sustentatoria que respalda las operaciones financieras, planes estratégicos, informes de auditoría, papeles de trabajo, informes de riesgos, expedientes de exempleados separados por destitución; cédulas presupuestarias, evaluaciones y liquidaciones presupuestarias, distributivos de remuneraciones, solicitudes de pago por anticipo de remuneraciones, horas extraordinarias y suplementarias, viáticos y subsistencias, subrogaciones, dietas, honorarios.

Diez años.- Expedientes de becarios nacionales e internacionales.

Quince años.- Expedientes de clientes de crédito educativo, a partir de la fecha de Concesión.

Permanente.- Leyes, reglamentos, manuales de procedimientos, operativos y de funcionamiento, instructivos, informes técnicos de relevancia, planes operativos anuales, presupuestos anuales, planes estratégicos, estados financieros anuales y otros similares, que permanecerán en las unidades correspondientes.

Se levantará un acta de eliminación de los documentos.

Se levantará un acta de baja de los documentos destruidos.

Ver anexo 11

REALIZADO POR: AMOY	FECHA: 01-09-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

APLICACIÓN DE INDICADORES

NOMBRE DEL INDICADOR	FACTORES CRÍTICOS DE ÉXITO	FORMULA DE CALCULO	FRECUENCIA	VALORES	%	INTERPRETACIÓN
NORMA 410-01 ORGANIZACIÓN INFORMÁTICA						
Porcentaje de problemas resueltos en la unidad de TICs, durante el año 2012.	Problemas generados y resueltos de forma oportuna en la unidad TICs.	$\frac{\text{Total problemas resueltos}}{\text{Total problemas generados en la unidad de TICs}}$	Anual	$\frac{470}{490} \times 100$	95,92%	En la unidad de TICs de la regional, se observa que los problemas generados en su mayor parte son resueltos de forma oportuna; sin embargo se debe propender a dar solución a todos los problemas presentados.
Porcentaje de cumplimiento de objetivos en el año 2012.	Cumplimiento adecuado de los objetivos planificados.	$\frac{\text{Total objetivos cumplidos}}{\text{Total objetivos planificados}}$	Anual	$\frac{8}{9} \times 100$	89%	La unidad de TICs debe esforzarse más para cumplir con los objetivos planificados.
NORMA 410-04 POLÍTICAS Y PROCEDIMIENTOS						
Porcentaje de políticas aplicadas en la unidad de TICs.	Cumplimiento adecuado y oportuno de todas las políticas establecidas para la unidad de TICs.	$\frac{\text{Total políticas aplicadas}}{\text{Total políticas establecidas}}$	Anual	$\frac{14}{14} \times 100$	100%	En la unidad de TICs existe un cumplimiento adecuado de las políticas establecidas.

REALIZADO POR: AMOY	FECHA: 22-09-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

Porcentaje de metas alcanzadas en la unidad de TICs.	Cumplimiento adecuado y oportuno de todas las metas definidas para la unidad de TICs.	$\frac{\text{Total metas alcanzadas}}{\text{Total metas definidas}}$	Anual	$\frac{88}{100} \times 100$	88%	El 88% indica que las metas no se han alcanzado en su totalidad por lo que se debe establecer mecanismos que permitan su cumplimiento.
Porcentaje de convenios alcanzados por la unidad de TICs.	Cumplimiento de todos los convenios definidos por la unidad de TICs.	$\frac{\text{Total convenios alcanzados}}{\text{Total convenios definidos}}$	Anual	$\frac{0}{0} \times 100$	0%	La unidad de TICs de la regional no realiza convenios.
NORMA 410- 09 MANTENIMIENTO Y CONTROL DE LA INFRAESTRUCTURA TECNOLÓGICA						
Porcentaje de actividades ejecutadas de mantenimiento establecidas en la unidad de TICs.	Actividades planificadas de mantenimiento efectuadas de acuerdo a lo establecido.	$\frac{\text{Total actividades ejecutadas de mantenimiento}}{\text{Total actividades planificadas de mantenimiento}}$	Anual	$\frac{2}{2} \times 100$	100%	Las actividades planificadas de mantenimiento son ejecutadas de forma correcta.
NORMA 410 -15 CAPACITACIÓN INFORMATICA						
Porcentaje de capacitaciones ejecutadas en la unidad de TICs.	Capacitaciones planificadas en la unidad de tics y efectuadas en el tiempo establecido.	$\frac{\text{Total capacitaciones ejecutadas en la unidad}}{\text{Total capacitaciones planificadas en la unidad}}$	Anual	$\frac{5}{6} \times 100$	83,33%	El 83,33% indica que las capacitaciones en la unidad de TICs se realizan pero no se cumple a cabalidad con lo planificado.

REALIZADO POR: AMOY	FECHA: 22-09-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

INDICADORES ADICIONALES						
Porcentaje de puntos obtenidos en la evaluación del personal de la unidad de TICs en el año 2012.	Cumplimiento de los puntos necesarios totales posibles en la evaluación.	$\frac{\text{Puntos obtenidos en la evaluación}}{\text{Puntos totales posibles en la evaluación}}$	Anual	$\frac{95,4}{100} \times 100$	95,4%	El personal de TICs de la entidad ha obtenido un 95,4% en la evaluación lo que indica que cuenta con conocimientos sólidos, sin embargo debe seguirse preparando para en la próxima evaluación obtener el puntaje máximo.
Porcentaje de tiempo medio con sistema no disponible en la entidad.	Tiempo total operativo disponible y desaprovechado por falla del sistema.	$\frac{\text{Tiempo con sistema no disponible}}{\text{Tiempo total operativo}}$	Semanal	$\frac{0,40}{40} \times 100$	1%	El tiempo medio con sistema no disponible representa el 1% lo cual indica que el 99% del tiempo total operativo la entidad dispone de sistema.
Porcentaje de tiempo medio con servidor no disponible en la entidad.	Tiempo total operativo disponible y desaprovechado por falla del servidor.	$\frac{\text{Tiempo con servidor no disponible}}{\text{Tiempo total operativo}}$	Semanal	$\frac{0}{40} \times 100$	0%	En la entidad se dispone del servidor todo el tiempo operativo

REALIZADO POR: AMOY	FECHA: 22-09-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

Porcentaje de quejas telefónicas resueltas durante la primera llamada por la unidad de TICs.	Quejas telefónicas resueltas de forma oportuna por la unidad de TICs.	$\frac{\text{Número de quejas telefónicas resueltas durante la primera llamada}}{\text{Número total de quejas telefónicas}}$	Diario	$\frac{5}{5} \times 100$	100%	Las quejas telefónicas receptadas son resueltas de forma oportuna durante la primera llamada.
Porcentaje de ordenadores disponibles en la entidad.	Funcionarios con ordenadores disponibles para ejecutar sus actividades.	$\frac{\text{Número de ordenadores}}{\text{Número de funcionarios}}$	Anual	$\frac{24}{25} \times 100$	96%	En la regional el 96% del personal dispone de computador y un funcionario que representa el 4% no dispone de ordenador para efectuar su actividad.
Porcentaje de impresoras disponibles en la entidad.	Unidades de la entidad que no disponen de impresoras.	$\frac{\text{Número de impresoras}}{\text{Número de unidades}}$	Anual	$\frac{7}{9} \times 100$	77,78%	El 77,78% de las unidades dispone de impresoras, lo cual refleja que existe un faltante de impresoras para cubrir las unidades existentes en la regional.

REALIZADO POR: AMOY	FECHA: 22-09-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

TERCERA ETAPA: DETERMINACIÓN DE HALLAZGOS

Entidad: IECE Regional 3 Riobamba
Área: TIC del IECE
Tipo de Auditoría: Auditoría Informática.
Fase: Determinación de Hallazgos

Objetivo: Determinar hallazgos en base a encuestas aplicadas, análisis de resultados, entrevistas realizadas y evidencia obtenida.

Nº	DESCRIPCIÓN	REF. PT.	ELABORADO POR:	FECHA
PROCEDIMIENTOS				
1	Realice determinación de hallazgos en base a los resultados obtenidos	HA	AMOY	01/10/13

TÍTULO I: Dependencia de la unidad de TICs Regional 3 Riobamba de la unidad de TICs matriz Quito.

CONDICIÓN: El IECE al tener su matriz en la ciudad de Quito y ser la entidad auditada una regional en la ciudad de Riobamba, no puede realizar ciertas actividades, entre estas tenemos:

No dispone de la facilidad de tomar decisiones y generar cambios de mejora tecnológica.

No promueve ni establece convenios con otras organizaciones o terceros a fin de promover y viabilizar el intercambio de información interinstitucional.

No interviene en la administración de proyectos tecnológicos.

Desconoce sobre la adquisición de software o soluciones tecnológicas.

Desconocimiento de aspectos en la adquisición y mantenimiento de la firma electrónica.

CRITERIO: Para poder aportar con cambios favorables y desenvolverse de una manera adecuada la unidad de TICs debe tener la facilidad de tomar decisiones y poder disponer de información que permitan mejorar su gestión.

CAUSA: Dependencia de la matriz

EFFECTO: La dependencia de la matriz no permite actuar de forma oportuna, se tiene que comunicar a la matriz y esperar respuesta para poder solucionar el problema causando retraso en las actividades.

CONCLUSIÓN: La dependencia de la matriz no permite actuar de forma oportuna en ciertas actividades, al igual que no se dispone de información sobre algunos aspectos informáticos.

RECOMENDACIÓN: Se sugiere a gerencia solicite a la matriz crear aplicativos intermedios que faciliten a la unidad de TICs tener acceso a información y permita realizar procesos para no depender siempre de la matriz y poder mejorar la gestión informática en la regional.

REALIZADO POR: AMOY	FECHA: 01-10-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

TÍTULO 2: Insuficiencia de personal en la unidad de TICs.

CONDICIÓN: La unidad de TICs cuenta con un solo funcionario para realizar las actividades de la unidad.

CRITERIO: Para desempeñar adecuadamente las actividades planificadas y ejecutarlas en el tiempo establecido se debe disponer de personal suficiente y competente.

CAUSA: La falta de un estudio para verificar si la carga laboral en la unidad de TICs es la adecuada.

EFECTO: Sobre carga laboral para el funcionario e incumplimiento de metas y actividades programadas para la unidad de TICs.

CONCLUSIÓN: La unidad de TICs no cuenta con personal suficiente para el desempeño de sus actividades, por ende no existe una rotación adecuada del personal y dependencia del funcionario en la entidad.

RECOMENDACIÓN: Se sugiere a gerencia contratar un funcionario para que ayude al funcionario existente a cumplir a cabalidad con las actividades asignadas a la unidad de TICs.

Este proceso se efectuara en base a al Art. 17.- Nombramiento, contratación y optimización del talento humano de la Ley orgánica de empresas públicas.

REALIZADO POR: AMOY	FECHA: 01-10-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

TÍTULO 3: La unidad de TICs no cuenta con un modelo de información organizacional.

CONDICIÓN: La unidad de TICs no cuenta con un modelo de información organizacional debido que esto lo realiza la matriz y lo ejecuta la unidad de comunicación.

CRITERIO: La unidad de TICs de la regional debe definir un modelo de información organizacional a fin de que sus procesos y procedimientos garanticen disponibilidad, integridad, exactitud y seguridad.

CAUSA: Dependencia de la matriz, lo realiza la unidad de comunicación y en la regional no se cuenta con esta unidad.

EFECTO: No dispone de un modelo de información organizacional adaptado a los procesos y procedimientos de la regional.

CONCLUSIÓN: La unidad de TICs no dispone de un modelo de información organizacional adaptado a sus procesos y procedimientos, solo dispone de un modelo de información organizacional general de la matriz.

RECOMENDACIÓN: Se sugiere a gerencia solicite al encargado de la unidad de TICs defina un modelo de información organizacional para la regional, tomando como referencia el modelo existente en la matriz y adapte a los procesos y procedimientos de la institución con la finalidad de garantizar disponibilidad, integridad, exactitud y seguridad.

REALIZADO POR: AMOY	FECHA: 01-10-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

TÍTULO 4: Inadecuada evaluación de los riesgos, vulnerabilidades y los requerimientos de seguridad.

CONDICIÓN: En la unidad de TICs falta reforzar los riesgos, vulnerabilidades y requerimientos de seguridad de la infraestructura tecnológica.

CRITERIO: Para un adecuado mantenimiento de la infraestructura tecnológica se debe considerar los riesgos, vulnerabilidades y requerimientos necesarios principalmente en las áreas críticas de la institución.

CAUSA: No se evalúa los riesgos, vulnerabilidades y los requerimientos de seguridad de la infraestructura tecnológica.

EFFECTO: Al no evaluarse los riesgos, vulnerabilidades y requerimientos de seguridad de la infraestructura tecnológica se pone en riesgo los servicios y bienes informáticos existentes en la entidad.

CONCLUSIÓN: En la unidad de TICs falta reforzar los riesgos, vulnerabilidades y requerimientos de seguridad de la infraestructura tecnológica.

RECOMENDACIÓN: Se sugiere a gerencia elaborar un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales con la finalidad de controlar los riesgos, vulnerabilidades y requerimientos de seguridad dando prioridad a aspectos críticos de la infraestructura tecnológica.

REALIZADO POR: AMOY	FECHA: 01-10-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

TÍTULO 5: Falta de medidas Seguridad Física adecuadas en la unidad de TICs.

CONDICIÓN: Su ubicación no es adecuada, no dispone de un control de acceso físico, no dispone de alarmas para detectar fuego, ni fuga de agua, no se ha adiestrado al personal en el manejo de los extintores y no dispone de una salida de emergencia.

CRITERIO: La unidad de TICs al ser un factor clave para el desempeño de las actividades en la entidad, debe contar con las condiciones necesarias para poder hacerlo y lograr así la eficiencia operativa.

CAUSA: Descuido de los involucrados y disponer de un espacio físico reducido en la entidad para la unidad de TICs.

EFFECTO: Riesgo de pérdidas y daños de los medios físicos y la información que se procesa mediante los sistemas informáticos.

CONCLUSIÓN: La unidad de TICs no cuenta con medidas de seguridad adecuadas que protejan y salvaguarden los medios físicos y la información generada en la unidad.

RECOMENDACIÓN: Se sugiere a gerencia:

Realizar modificaciones a la unidad de TICs de acuerdo al espacio existente en la entidad para acoplarlo de mejor manera.

Incorporar un control de acceso físico al ingreso de la unidad de TICs.

Implementar un circuito cerrado de vigilancia.

Colocar alarmas para detectar fuego o fugas de agua.

Adiestrar al personal sobre el manejo de los extintores.

REALIZADO POR: AMOY	FECHA: 01-10-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

TÍTULO 6: Contenido y manejo del plan de contingencias poco satisfactorio.

CONDICIÓN: La unidad de TICs dispone de un plan de contingencias pero existen debilidades en el contenido y en el empleo del mismo.

CRITERIO: al momento de suscitarse alguna eventualidad se debe conocer cómo actuar y que pasos seguir, para ello es necesario contar con un plan de contingencias adecuado.

CAUSA: Plan de contingencias débil y la inadecuada difusión del mismo en la entidad.

EFECTO: Desconocimiento de las acciones a tomar en caso de una emergencia.

CONCLUSIÓN: el plan de contingencias existente en la entidad no dispone de un plan de respuesta a los riesgos, no cuenta con un plan de recuperación de desastres, no se ha designado un comité con nombres y roles específicos para ejecutar las funciones de contingencia en caso de suscitarse una emergencia, no es difundido entre el personal responsable de su ejecución, y no es sometido a pruebas, entrenamiento y evaluaciones periódicas.

RECOMENDACIÓN: Se sugiere a gerencia modifique el plan de contingencias e incorpore un plan de respuesta a los riesgos, un plan de recuperación de desastres, designe un comité con nombres y roles específicos el cual sea difundido y sometido a pruebas y evaluaciones periódicas para ejecutar las funciones de contingencia en caso de suscitarse una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.

REALIZADO POR: AMOY	FECHA: 01-10-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

TÍTULO 6: Insuficiencia de impresoras en la regional.

CONDICIÓN: En la regional existen nueve unidades y existen solamente siete impresoras.

CRITERIO: Para poder ejecutar sus actividades y evitar pérdida de tiempo en trasladarse a otra unidad se debería proporcionar a cada unidad de una impresora.

CAUSA: Descuido de los funcionarios al no sugerir a gerencia la adquisición de impresoras para las unidades faltantes.

EFECTO: Perdida de tiempo en trasladarse a otra unidad al no disponer de una impresora, retraso en las actividades, posibles pérdidas y confusión de documentos.

CONCLUSIÓN: En la regional no existen suficientes impresoras para cubrir con las unidades existentes en la entidad.

RECOMENDACIÓN: Se sugiere a gerencia adquiera dos impresoras e instale las mismas en las unidades que no disponen para facilitar su trabajo y evitar posible pérdida de documentos.

REALIZADO POR: AMOY	FECHA: 01-10-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

CUARTA ETAPA: COMUNICACIÓN DE RESULTADOS

PROGRAMA DE AUDITORÍA

Entidad: IECE Regional 3 Riobamba
Tipo de Auditoría: Auditoría Informática
Fase: Comunicación de Resultados

Objetivo: Dar a conocer los hallazgos encontrados durante la evaluación en la utilización y aprovechamiento de tecnologías de información.

N°	DESCRIPCIÓN	REF: PT	ELABORADO POR	FECHA
PROCEDIMIENTOS GENERALES				
1	Elabore Carta de Presentación		AMOY	05/11/13
2	Elabore el informe final de Auditoría.		AMOY	05/11/13
3	Elabore el Acta de Convocatoria		AMOY	05/11/13
4	Realice Convocatoria		AMOY	06/11/13

CARTA DE PRESENTACIÓN

Riobamba 22 de Diciembre del 2013.

Ingeniera

Econ. Yesenia Díaz

GERENTE DEL IECE REGIONAL 3 RIOBAMBA

Presente

De mi consideración:

Se ha realizado la Auditoria Informática al Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba, correspondiente al período del 01 de Enero al 31 de Diciembre del 2012.

El análisis se realizó de acuerdo con las Normas de control interno emitidas por la Contraloría General del Estado en lo referente tecnologías de información y comunicación. La evaluación incluye la utilización y aprovechamiento de tecnologías de información y comunicación TICs y gestión de la informática.

Debido a la naturaleza del estudio y de los componentes evaluados los resultados de la auditoría se encuentran en las conclusiones y recomendaciones del presente informe.

Atentamente,

Sr. Alex Obando

INFORME CONFIDENCIAL

Riobamba 22 de Diciembre del 2013.

Emisión del informe de Auditoría Informática.

A la gerencia del INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS (IECE) REGIONAL 3 RIOBAMBA

1. Se ha efectuado la Auditoría Informática al Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba, correspondiente al período del 01 de Enero al 31 de Diciembre del 2012, en cuanto al aprovechamiento y utilización de las TICs y gestión de la informática, mi responsabilidad consiste en expresar una opinión sobre los mismos en base a la práctica de la auditoría.

2. El análisis se realizó de acuerdo con las Normas de control interno emitidas por la Contraloría General del Estado en lo referente a tecnologías de información y comunicación.

La gran mayoría de los síntomas percibidos a lo largo de la Auditoría Informática obedecen a la dependencia de la unidad de TICs de la regional con la matriz (Quito) no permite actuar de forma oportuna ni disponer de información sobre algunos aspectos informáticos por lo que se tiene que comunicar a la matriz y esperar respuesta para poder solucionar el problema causando retraso en los procesos. La unidad de TICs no cuenta con personal suficiente para el desempeño de sus actividades, por ende no existe una rotación adecuada del personal y existe dependencia del funcionario en la entidad, no dispone de un modelo de información organizacional, la ubicación no es adecuada, no dispone de un control de acceso físico, no dispone de alarmas para detectar fuego, ni fuga de agua, no se ha adiestrado al personal en el manejo de los extintores y no dispone de una salida de emergencia; la unidad de TICs dispone de un plan de contingencias pero existen debilidades en el contenido y en el empleo del mismo; la regional no dispone de suficientes impresoras.

3. En mi opinión, los aspectos mencionados en el párrafo anterior son debilidades que se deben mejorar a través de la toma de decisiones en base en las recomendaciones emitidas en el presente informe.

Sr. Alex Obando

INFORME DE AUDITORÍA INFORMÁTICA

CAPITULO I

Motivo del examen.

El trabajo se realizó por la razón que en el Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba, no se ha realizado una Auditoría Informática que evalúe el aprovechamiento, utilización de TICs y la Gestión Informática. Considerando esta situación he desarrollado el proyecto de tesis en la entidad con énfasis y mayor estudio en la unidad de TICs de manera que el beneficio sea para las dos partes involucradas.

Objetivo General.

Realizar una Auditoría Informática al Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba, para mejorar los sistemas de gestión de tecnologías de la información y comunicación periodo 2012.

Objetivos Específicos.

Determinar si existe establecidas políticas de cambio de claves de acceso a los sistemas de información en la entidad.

Verificar si existen medidas de seguridad física que permita proteger y salvaguardar los bienes de la entidad.

Determinar si existe una planificación de actividades en la unidad de TICs, planes de contingencia, indicadores de desempeño.

Alcance.

La Auditoria Informática al Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba, comprendió el estudio y análisis de aspectos relacionados con la seguridad física, utilización y aprovechamiento de tecnologías de información y comunicación y gestión de la informática.

Base Legal.

El Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba es una institución que renueva cada día su responsabilidad social de apoyar el afán de superación

de la población estudiantil ecuatoriana, pues mediante el crédito educativo y las becas, se logra el sendero de un Ecuador próspero y diferente.

El IECE para el desarrollo de sus actividades cuenta con las siguientes disposiciones legales, reglamentarias y demás disposiciones internas:

Crédito

- Reglamento de Crédito Educativo.
- Manual de Gestión de Crédito.
- Manual de Procedimiento Coactivo.
- Reglamento para el Ejercicio de la Jurisdicción Coactiva.
- Reforma al Reglamento de la Jurisdicción Coactiva.

Becas

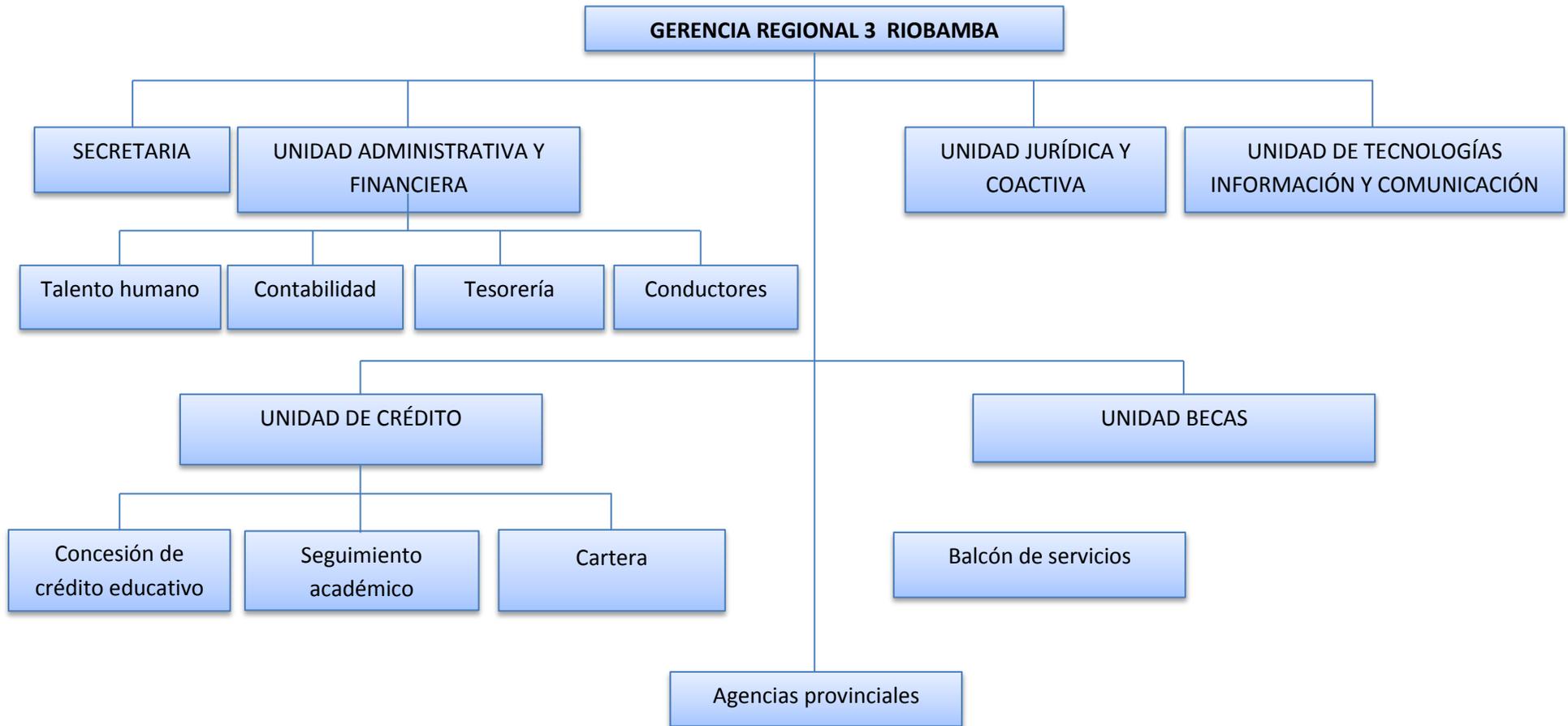
- Reglamento Becas Hijos Combatientes del CENEPA
- Instructivo para la Ejecución de Becas ECORAE
- Reforma al Instructivo para la Ejecución del Subprograma Monseñor Leonidas Proaño componente Cuba.
- Instructivo del Subprograma Eloy Alfaro componente Zamorano.
- Ley de Creación de la Beca Estudiantil de Entrenamiento.
- Reglamento Ejecución de Becas Universidad Sin Fronteras Perú-Ecuador.
- Reglamento Funcionamiento Comisión Mixta de Selección de Becarios.

Generales

- Constitución Política del Estado.
- Reglamento de Atribuciones y Deberes del Directorio.
- Reglamento de Contrataciones.
- Reglamento del Comité de Auditoria.
- Reglamento para la Selección y Eliminación de Documentos.
- Manual de Prevención de Lavado de Activos.
- Reglamento de Administración de RRHH.
- Reglamento para el Funcionamiento del Comité de Cumplimiento.
- Reforma al Reglamento para el Funcionamiento del Comité de Cumplimiento del IECE.

Organigrama IECE Regional 3 Riobamba

Figura 5: Organigrama Institucional



Fuente: Reglamento Orgánico de Gestión por Procesos del Instituto Ecuatoriano de Crédito Educativo y Becas

Elaborado por: El Autor de tesis

RESULTADOS DEL EXAMEN

CAPITULO II

Dependencia de la unidad de TICs Regional 3 Riobamba de la unidad de TICs matriz Quito.

CONCLUSIÓN: La dependencia de la matriz no permite actuar de forma oportuna en ciertas actividades, al igual que no se dispone de información sobre algunos aspectos informáticos.

RECOMENDACIÓN: Se sugiere a gerencia solicite a la matriz crear aplicativos intermedios que ayuden y faciliten a la unidad de TICs a tener acceso a datos que permitan mejorar la gestión informática en la regional.

Insuficiencia de personal en la unidad de TICs.

CONCLUSIÓN: La unidad de TICs no cuenta con personal suficiente para el desempeño de sus actividades, por ende no existe una rotación adecuada del personal y dependencia del funcionario en la entidad.

RECOMENDACIÓN: Se sugiere a gerencia contratar un funcionario para que ayude al funcionario existente a cumplir a cabalidad con las actividades asignadas a la unidad de TICs.

Este proceso se efectuara en base a al Art. 17.- Nombramiento, contratación y optimización del talento humano de la Ley orgánica de empresas públicas.

La unidad de TICs no cuenta con un modelo de información organizacional.

CONCLUSIÓN: La unidad de TICs no dispone de un modelo de información organizacional adaptado a sus procesos y procedimientos, solo dispone de un modelo de información organizacional general de la matriz.

RECOMENDACIÓN: Se sugiere a gerencia solicite al encargado de la unidad de TICs defina un modelo de información organizacional para la regional, con la finalidad de facilitar su uso y compartición.

Inadecuada evaluación de los riesgos, vulnerabilidades y los requerimientos de seguridad.

CONCLUSIÓN: En la unidad de TICs falta reforzar los riesgos, vulnerabilidades y requerimientos de seguridad de la infraestructura tecnológica.

RECOMENDACIÓN: Se sugiere a gerencia elaborar un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales con la finalidad de controlar los riesgos, vulnerabilidades y requerimientos de seguridad dando prioridad a aspectos críticos de la infraestructura tecnológica.

Falta de medidas Seguridad Físicas adecuadas en la unidad de TICs.

CONCLUSIÓN: la unidad de TICs no cuenta con medidas de seguridad adecuadas que protejan y salvaguarden los medios físicos y la información generada en la unidad.

RECOMENDACIÓN: Se sugiere a gerencia:

Realizar modificaciones a la unidad de TICs de acuerdo al espacio existente en la entidad para acoplarlo de mejor manera.

Incorporar un control de acceso físico al ingreso de la unidad de TICs.

Colocar alarmas para detectar fuego o fugas de agua.

Adiestrar al personal sobre el manejo de los extintores.

Contenido y manejo del plan de contingencias poco satisfactorio

CONCLUSIÓN: el plan de contingencias existente en la entidad no dispone de un plan de respuesta a los riesgos, no cuenta con un plan de recuperación de desastres, no se ha designado un comité con nombres y roles específicos para ejecutar las funciones de contingencia en caso de suscitarse una emergencia, no es difundido entre el personal responsable de su ejecución, y no es sometido a pruebas, entrenamiento y evaluaciones periódicas.

RECOMENDACIÓN: Se sugiere a gerencia modifique el plan de contingencias e incorpore un plan de respuesta a los riesgos, un plan de recuperación de desastres, designe un comité con nombres y roles específicos el cual sea difundido y sometido a pruebas y evaluaciones periódicas para ejecutar las funciones de contingencia en caso de suscitarse una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.

Insuficiencia de impresoras en la regional.

CONCLUSIÓN: En la regional no existen suficientes impresoras para cubrir con las unidades existentes en la entidad.

RECOMENDACIÓN: Se sugiere a gerencia compre dos impresoras e instale las mismas en las unidades que no disponen para facilitar su trabajo y evitar posible pérdida de documentos.

Convocatoria de conferencia final

Ingeniera

Econ. Yesenia Díaz

GERENTE DEL IECE REGIONAL 3 RIOBAMBA

Presente

De mi consideración:

De conformidad con lo dispuesto en los artículos 90 de la Ley Orgánica de la Contraloría General del Estado y 23 de su reglamento convoco a usted a la conferencia final de comunicación de resultados mediante la lectura del borrador del informe de la Auditoría Informática al Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba, para mejorar los Sistemas de Gestión de Tecnologías de la Información y Comunicación, período 2012 mediante orden de trabajo 001 de fecha quince de julio del dos mil trece.

La diligencia se llevará a cabo en la Unidad Administrativa – Financiera de la entidad el día 22 de Diciembre del 2013. En caso de no poder asistir personalmente agradeceré notificar por escrito, indicando los nombres, apellidos y número de cédula de ciudadanía de la persona que actuará en su representación.

Atentamente

Sr. Alex Obando

ACTA DE CONFERENCIA FINAL DE COMUNICACIÓN DE RESULTADOS CONTENIDOS EN EL BORRADOR DEL INFORME DE LA AUDITORÍA INFORMÁTICA AL INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS (IECE) REGIONAL 3 RIOBAMBA, PERIODO 2012.

En la ciudad de Riobamba, provincia de Chimborazo, a los veintidós días del mes de diciembre del dos mil trece, a las diez horas, el suscrito: Sr. Alex Mauricio Obando Yumisaca, se constituyen en la Unidad Administrativa - Financiera de la entidad, con el objeto de dejar constancia de la lectura del Borrador del Informe de Auditoría Informática al Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba, para mejorar los sistemas de Gestión de Tecnologías de la información y comunicación, período 2012 que realizado de conformidad a la carta a gerencia enviada quinde de julio del dos mil trece.

Se convocó mediante oficio a los funcionarios, para que asistan a la presente diligencia.

Al efecto, en presencia de los abajo firmantes, se procedió a la lectura del borrador del informe, se analizaron y discutieron los resultados de la Auditoría, constantes en los comentarios, conclusiones y recomendaciones.

Para constancia de lo actuado, las personas asistentes suscriben la presente acta en dos ejemplares de igual tenor.

Nombre y apellidos	Cargo	N° de cédula	Firma
Econ. Yesenia Díaz	Gerente		
Ing. Marcelo Monar	Funcionario Unidad de TICS		

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- La evaluación y revisión de la situación actual al Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba permitió conocer cuáles son las necesidades que esta posee y como se denota la realización de una auditoría informática.
- La auditoría informática formulada y presentada ha generado opiniones sobre los aspectos gerenciales y operativos, haciendo hincapié en el grado de efectividad y eficiencia sobre el manejo de los recursos informáticos, mediante la evaluación de control interno, controles operativos, y algunos aspectos relacionados con el funcionamiento general de la institución.
- Las normas de control interno referente a las TICs y la guía metodológica empleadas en la realización de la auditoría informática a la institución, permitió desarrollar un trabajo de campo adecuado a través del empleo de métodos y técnicas que reflejaron de forma objetiva la situación de la entidad.
- Una vez realizada la auditoría informática se pudo determinar que la unidad de TICs no dispone de cierta información como: adquisición del software, firmas electrónica y administración de proyectos tecnológicos; existiendo también dependencia de la matriz debido que al momento que se suscita una falla en el sistema no puede actuar y tiene que esperar respuesta de la matriz ocasionando retraso en las actividades de la regional.
- Los hallazgos encontrados y mencionados en el informe de auditoría como: la dependencia de la matriz, insuficiencia de personal, falta de un modelo de información organizacional, falta de seguridades, plan de contingencia débil; son debilidades que afectan al buen desenvolviendo de la unidad de TICs sin embargo se plantearon las recomendaciones pertinentes para mejorarlas.

- Mediante la realización de la auditoría informática se pudo determinar que la utilización y aprovechamiento de las TICs, a excepción de los hallazgos presentados en el informe de auditoría se han realizado eficientemente según las normas de control interno referente a tecnologías de información y comunicación.

5.2 RECOMENDACIONES

- El presente trabajo constituye una fuente de consulta y referencia didáctica para docentes, estudiantes y personas que necesiten conceptos de auditoría informática.
- La gerencia debe potencializar y aprovechar las fortalezas y oportunidades existentes en la institución y contrarrestar las debilidades y amenazas encontradas en análisis situacional.
- Solicitar a la matriz crear aplicativos intermedios que faciliten a la unidad de TICs tener acceso a información y permita realizar procesos para no depender siempre de la matriz y poder mejorar la gestión informática en la regional.
- Realizar las correcciones correspondientes dentro de cada componente para mitigar riesgos y disminuir las debilidades encontradas.
- Dar seguimiento al cumplimiento de las recomendaciones emitidas en el informe de auditoría, para garantizar la correcta utilización y aprovechamiento de las TICs en la institución.

RESUMEN

La presente investigación es una Auditoría Informática aplicada al Instituto Ecuatoriano de Crédito Educativo y Becas (IECE) Regional 3 Riobamba, para mejorar los sistemas de gestión de tecnologías de información y comunicación, período 2012. Está enmarcada en el desarrollo y análisis de la utilización y aprovechamiento de tecnologías de información y comunicación (TICs).

Para el desarrollo de la Auditoría Informática se empezó con el conocimiento preliminar de la entidad de manera que permitió realizar una adecuada planificación que integre los programas correspondientes a la unidad sujeta de análisis, a través de aplicación de técnicas y procedimientos de auditoría. Se toma como referencia las normas de control interno referente a tecnologías de información y comunicación de la Contraloría General del Estado (CGE).

Como resultado de la Auditoría Informática se tiene; dependencia de la unidad de TICs de la regional con la matriz (Quito) debido a que no permite actuar de forma oportuna, ni disponer de información sobre algunos aspectos informáticos, insuficiencia de personal, no cuenta con un modelo de información organizacional, la ubicación no es adecuada, no tiene un control de acceso físico, no dispone de alarmas para detectar fuego, ni fuga de agua, no se ha adiestrado al personal en el manejo de los extintores y no dispone de una salida de emergencia; la unidad de TICs cuenta con un plan de contingencias pero existen debilidades en el contenido y en el empleo del mismo; la regional no dispone de suficientes impresoras.

Se recomienda tomar en cuenta los aspectos estipulados en el informe de auditoría para mejorar la gestión de la tecnología de información y comunicación en la entidad.

SUMMARY

The present investigation is an Informatic Auditing applied to the IECE (Instituto Ecuatoriano de Crédito Educativo y Becas) Regional 3 Riobamba, to improve the information and communication technology management, period 2012. It is framed in the development and analysis of the using and exploitation of technologies of information and communication (TICs).

For the development of the Informatic Auditing was begun with the preliminary recognizing of the entity in way that permitted to make an adequate planning that integrates the corresponding programs to the unit subjected to analysis, through the application of techniques and procedures of auditing. It is taken as reference the internal control norms related to technologies of information and communication belonging to the State General Controller (CGE).

As a result of the Informatics Auditing has dependency of the unit of TICs from the regional with the subsidiary (Quito) due to not permits to act in an opportunistic way, neither dispose of information about some informatics aspects, insufficient staff who do not have an organizational information model; the location, which is inappropriate, nor available a physical control access, neither alarms to detect fire, nor water leaks, nor it has been trained the staff in the management of fire extinguishers and neither it has an emergency exit; the unit of TICs counts with a contingency plan, but it exists weaknesses in the content and employment of the same; the regional does not possess enough printers.

It is recommended to take into account the stipulated aspects in the auditing report to improve the management of the technology of information and communication in the entity.

BIBLIOGRAFÍA

- Cadena , N. (2011). *Módulo de Auditoría Informática*. Riobamba: Obra Inédita.
- De la Peña G., A. (2008). *Auditoría Un enfoque Práctico*. Madrid, España: Editorial Paraninfo.
- Esparza, F. (2010). *Auditoría de Gestión*. Riobamba.
- Fred, D. (1997). *Conceptos de Administración Estratégica*. Mexico: Prentice - Hall Hispanoamericana.
- Hernández, E. (1996). *Auditoría Informática Un Enfoque Metodológico*. México: Continental.
- Kell, W., & Zieger, R. (1988). *Auditoría Moderna*. México: Continental.
- Madariaga Gorocica, J. (2004). *Manual Práctico de Auditoría*. España: Ediciones Deusto.
- Muñoz Razo, C. (2002). *Auditoría en Sistemas Computacionales*. México: Cámara Nacional de la Industria Editorial Mexicana.
- Ortiz, J., & Ortiz, A. (2002). *Auditoría Integral con Enfoque al Control de Gestión Administrativo y Financiero*. Quito: kimpres Ltda.
- Piattini del Peso, E. (2005). *Auditoría Informática un Enfoque Práctico (Vol. 2)*. Colombia.
- Slosse, C.A., Gordiez, J.C., Giordano Silva. (1999). *Auditoría un nuevo enfoque empresarial*. Buenos Aires: Ediciones MACHI.

LINKOGRAFÍA

- IECE. (15 de Octubre de 2013). *La institución Leyes y Reglamentos*. Recuperado el 21 de Enero de 2013, de Instituto Ecuatoriano de Crédito Educativo y Becas:
<http://www.eice.fin.ec/institucion/leyes-y-reglamentos>
- IECE. (15 de Octubre de 2013). *La institución Misión. Visión*. Recuperado el 21 de Enero de 2013, de Instituto Ecuatoriano de Crédito Educativo y Becas:
<http://www.iece.fin.ec/institución/misión-visión>
- Instituto Ecuatoriano de Crédito Educativo y Beca, I. (miercoles de octubre de 2013). *INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS*. Recuperado el 21 de enero de 2013, de La Institución. Historia:
www.iece.fin.ec/institucion/historia/creacion
- MONOGRAFIAS.COM. (Febrero de 2009). *Características de la Auditoría*. Recuperado el 20 de Enero de 2013, de
<http://www.monografias.com/trabajos32/auditoria.shtml>.
- VANDAMA. N., LESCAY. M., CASTILLO. G., y GARCIA. F. . (2 de febrero de 2002). *Auditoría Informática en ETECSA* . Recuperado el 21 de Marzo de 2013, de Auditoría Informática en ETECSA : <http://espejos.unesco.org.uy/simplac2002/ponencias/Segunrm%eltica/VIR024.doc>
- XIMENEZ, M. (Marzo de 2011). Auditoría efectuada a la jefatura de recursos humanos. *Tesis Universidad Particular de Loja*. Loja:
http://www.contraloriaibague.gov.co/index.php?option=com_cintent&view=article&id=66&Itemid=71.



PAPELES DE TRABAJO

EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO TICS

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO**

Área: TIC del IECE
Componente: Organización informática

MOTIVO DEL EXAMEN: Conocer si la entidad esta acoplada en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, y disponga de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional.

N°	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
1	¿La entidad cuenta con un marco de trabajo para procesos de tecnología de información?	x			
2	¿El marco de trabajo para procesos de tecnología de información existente asegura la transparencia y control de las actividades de la entidad?	x			
3	¿Cuenta esta unidad con un responsable que regule y estandarice los temas tecnológicos?	x			
4	¿La unidad de TICS se encuentra en una estructura organizacional que le permita efectuar actividades de asesoría y apoyo a la alta dirección y unidades usuarias?	x			
5	¿La unidad dispone de la facilidad de tomar decisiones y generar cambios de mejora tecnológica?		x		Depende de la coordinación con la matriz.
6	¿La unidad garantiza su independencia respecto con las otras áreas de la entidad?	x			
7	¿Se revisa de forma periódica la estructura organizacional de la tecnología de información?	x			
8	¿La unidad realiza ajustes en las estrategias internas para cumplir con los objetivos planteados y soporten los avances tecnológicos?	x			
TOTAL		7	1	0	

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
MATRIZ DE PONDERACIÓN

Nº	COMPONENTE	PONDERACIÓN	CALIFICACIÓN
1	¿La entidad cuenta con un marco de trabajo para procesos de tecnología de información?	10	10
2	¿El marco de trabajo para procesos de tecnología de información existente asegura la transparencia y control de las actividades de la entidad?	10	10
3	¿Cuenta esta unidad con un responsable que regule y estandarice los temas tecnológicos?	10	10
4	¿La unidad de TICs se encuentra en una estructura organizacional que le permita efectuar actividades de asesoría y apoyo a la alta dirección y unidades usuarias?	10	10
5	¿La unidad dispone de la facilidad de tomar decisiones y generar cambios de mejora tecnológica?	10	0
6	¿La unidad garantiza su independencia respecto con las otras áreas de la entidad?	10	10
7	¿Se revisa de forma periódica la estructura organizacional de la tecnología de información?	10	8
8	¿La unidad realiza ajustes en las estrategias internas para cumplir con los objetivos planteados y soporten los avances tecnológicos?	10	8
TOTAL		80	66

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

DETERMINACIÓN DEL NIVEL DE RIESGO

$$\text{CONFIANZA PONDERADA} = \frac{\text{Calificación Total}}{\text{Ponderación Total}} * 100$$

$$\text{CONFIANZA PONDERADA} = \frac{66}{80} * 100$$

$$\text{CONFIANZA PONDERADA} = 82,5\%$$

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

RESULTADO:

- **CONFIANZA:** Alta 82,5
- **RIESGO:** Bajo 17,5

Análisis: La institución dispone de una unidad que se encargue de regular y estandarizar los temas tecnológicos y este acoplada en un marco de trabajo para procesos de tecnología de información; sin embargo se encontró que la unidad no dispone de la facilidad de tomar decisiones y generar cambios de mejora tecnológica debido a que la unidad depende de la coordinación con la matriz.

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO**

Área: TIC del IECE
Componente: Segregación de funciones

MOTIVO DEL EXAMEN: Conocer si el personal de la unidad de TICs, cuenta con funciones y responsabilidades claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo.

Nº	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
1	¿Las funciones y responsabilidades del personal de tecnología de información son claramente definidas y formalmente comunicadas?	x			
2	¿Se realiza la supervisión de roles y funciones del personal que labora en la unidad de TICs?	x			
3	¿Los puestos de trabajo que conforman la unidad de tecnología de información están debidamente documentados y aprobados?	x			
4	¿Se realiza una evaluación del desempeño del personal de unidad de tecnología de información?	x			
5	¿La unidad de TICs cuenta con el personal suficiente para realizar sus actividades?		x		No cuenta con personal suficiente.
TOTAL		4	1	0	

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
MATRIZ DE PONDERACIÓN**

Nº	COMPONENTE	PONDERACIÓN	CALIFICACIÓN
1	¿Las funciones y responsabilidades del personal de tecnología de información son claramente definidas y formalmente comunicadas?	10	8
2	¿Se realiza la supervisión de roles y funciones del personal que labora en la unidad de TICs?	10	10
3	¿Los puestos de trabajo que conforman la unidad de tecnología de información están debidamente documentados y aprobados?	10	10
4	¿Se realiza una evaluación del desempeño del personal de unidad de tecnología de información?	10	8
5	¿La unidad de TICs cuenta con el personal suficiente para realizar sus actividades?	10	5
TOTAL		50	39

DETERMINACIÓN DEL NIVEL DE RIESGO

$$CONFIANZA PONDERADA = \frac{Calificación\ Total}{Ponderación\ Total} * 100$$

$$CONFIANZA PONDERADA = \frac{39}{50} * 100$$

$$CONFIANZA PONDERADA = 78\%$$

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

RESULTADO:

- **CONFIANZA:** 78% Alta
- **RIESGO:** 22% Bajo

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

Análisis: El personal que labora en la institución en la unidad de TICs, es solo una persona por lo que las funciones y responsabilidades que debe cumplir están claramente definidas y formalmente comunicadas sin embargo se detectó que el personal que labora en la unidad de TICs no es el suficiente.

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO**

Área: TIC del IECE

Componente: Plan informático estratégico de tecnología

MOTIVO DEL EXAMEN: Conocer si la unidad de TICs elabora e implementa un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos.

Nº	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
1	¿La unidad de tecnología de información dispone de un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos?	x			
2	¿El plan informático estratégico está alineado con el plan estratégico institucional y este con el Plan Nacional de Desarrollo y las políticas públicas de gobierno?	x			
3	¿El plan informático estratégico permite la definición de planes operativos de tecnología de Información?	x			
4	¿EL plan estratégico y los planes operativos de tecnología de información son analizados y aprobados por la máxima autoridad de la institución?	x			
5	¿EL plan estratégico y los planes operativos de tecnología de información son actualizados de manera permanente?	x			
6	¿El P.E y los P.O de la T.I son monitoreados y evaluados de forma trimestral?	x			
TOTAL		6	0	0	

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
MATRIZ DE PONDERACIÓN**

Nº	COMPONENTE	PONDERACIÓN	CALIFICACIÓN
1	¿La unidad de tecnología de información dispone de un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos?	10	8
2	¿El plan informático estratégico está alineado con el plan estratégico institucional y este con el Plan Nacional de Desarrollo y las políticas públicas de gobierno?	10	8
3	¿El plan informático estratégico permite la definición de planes operativos de tecnología de Información?	10	8
4	¿EL plan estratégico y los planes operativos de tecnología de información son analizados y aprobados por la máxima autoridad de la institución?	10	10
5	¿EL plan estratégico y los planes operativos de tecnología de información son actualizados de manera permanente?	10	10
6	¿El P.E y los P.O de la T.I son monitoreados y evaluados de forma trimestral?	10	10
TOTAL		60	54

DETERMINACIÓN DEL NIVEL DE RIESGO

$$CONFIANZA PONDERADA = \frac{\text{Calificación Total}}{\text{Ponderación Total}} * 100$$

$$CONFIANZA PONDERADA = \frac{54}{60} * 100$$

$$CONFIANZA PONDERADA = 90\%$$

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

RESULTADO:

- **CONFIANZA:** 90 % Alta
- **RIESGO:** 10% Bajo

Análisis: La unidad de TICs dispone de un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos; el mismo que esta alineado con el plan estratégico institucional y este con el Plan Nacional de Desarrollo y las políticas públicas de gobierno los mismos que son evaluados de forma trimestral.

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO**

Área: TIC del IECE
Componente: Políticas y procedimientos

MOTIVO DEL EXAMEN: Conocer si la máxima autoridad de la entidad aprueba las políticas y procedimientos que permitan organizar apropiadamente la unidad de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria.

N°	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
1	¿Las políticas y procedimientos de la unidad de tecnología de información son aprobadas por la máxima autoridad de la institución?	x			
2	¿Las políticas y procedimientos existentes permitan organizar apropiadamente la unidad de tecnología de información?	x			
3	¿Las políticas y procedimientos existentes permitan contar con talento humano calificado en la unidad de tecnología de información?	x			
4	¿La unidad de tecnología de información define, documenta y difunde las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la entidad?	x			
5	¿Se han establecido sanciones administrativas a que hubiere lugar si no se cumplieran con las políticas y procedimientos establecidos?	x			
6	¿Las políticas y procedimientos definidos consideran temas como la calidad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas, mensajería de datos, legalidad del software?	x			
7	¿Las políticas y procedimientos están alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información?	x			Responsabilidad de TICs Matriz.
8	¿Existen procedimientos de comunicación, difusión y coordinación entre las funciones de tecnología de información y las funciones propias de la organización?	x			
9	¿La unidad de tecnología de información		x		Esta es

	promueve y establece convenios con otras organizaciones o terceros fin de promover y viabilizar el intercambio de información interinstitucional?				responsabilidad de la unidad de comunicación en coordinación con la gerencia regional y la gerencia general.
TOTAL		8	1	0	

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
MATRIZ DE PONDERACIÓN**

Nº	PREGUNTAS	PONDERACIÓN	CALIFICACIÓN
1	¿Las políticas y procedimientos de la unidad de tecnología de información son aprobadas por la máxima autoridad de la institución?	10	10
2	¿Las políticas y procedimientos existentes permitan organizar apropiadamente la unidad de tecnología de información?	10	5
3	¿Las políticas y procedimientos existentes permitan contar con talento humano calificado en la unidad de tecnología de información?	10	10
4	¿La unidad de tecnología de información define, documenta y difunde las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la entidad?	10	8
5	¿Se han establecido sanciones administrativas a que hubiere lugar si no se cumplieran con las políticas y procedimientos establecidos?	10	10
6	¿Las políticas y procedimientos definidos consideran temas como la calidad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas, mensajería de datos, legalidad del software?	10	8
7	¿Las políticas y procedimientos están alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información?	10	10
8	¿Existen procedimientos de comunicación, difusión y coordinación entre las funciones de tecnología de información y las funciones propias de la organización?	10	8
9	¿La unidad de tecnología de información promueve y establece convenios con otras organizaciones o terceros fin de promover y viabilizar el intercambio de información interinstitucional?	10	0
TOTAL		90	69
		REALIZADO POR: AMOY	FECHA: 27-07-2013
		REVISADO POR: BNCO	FECHA: 17-08-2013

DETERMINACIÓN DEL NIVEL DE RIESGO

$$CONFIANZA PONDERADA = \frac{\text{Calificación Total}}{\text{Ponderación Total}} * 100$$

$$CONFIANZA PONDERADA = \frac{69}{90} * 100$$

$$CONFIANZA PONDERADA = 76,67\%$$

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

RESULTADO:

- **CONFIANZA:** Alta 76,67 %
- **RIESGO:** Bajo 23,33 %

Análisis: Las políticas y procedimientos de la unidad de tecnología de información son aprobadas por la máxima autoridad de la institución permitiendo su organización adecuada, cuenta con talento humano calificado, se han establecido sanciones administrativas en caso de que no se cumplan con las políticas y procedimientos establecidos, sin embargo falta definir subprocesos que desconcentren la matriz de la regional para poder tener un mejor control en la institución.

La unidad de tecnología de información no participa en promover y establecer convenios con otras organizaciones o terceros a fin de promover y viabilizar el intercambio de información interinstitucional, pero esto, si se lo ejecuta en la matriz (Quito) de la institución, en la unidad de comunicación sin embargo en la regional 3 no dispone una unidad de comunicación.

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO**

Área: TIC del IECE
Componente: Modelo de información organizacional

MOTIVO DEL EXAMEN: Conocer si la unidad de TICs define el modelo de información de la organización a fin de que se facilite la creación, uso y compartición de la misma; y se garantice su disponibilidad, integridad, exactitud y seguridad sobre la base de la definición e implantación de los procesos y procedimientos correspondientes.

Nº	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
1	¿La unidad de tecnología de información cuenta con un modelo de información organizacional?		x		Esto realiza la unidad de comunicación Apoyada con TICs.
2	¿El modelo de información organizacional es actualizado y documentado de forma permanente?		x		Es competencia de la Unidad de comunicación.
3	¿El modelo de información organizacional facilita la incorporación de las aplicaciones y procesos institucionales de forma transparente?	x			
4	¿Se genera un proceso de clasificación de los datos para especificar y aplicar niveles de seguridad y propiedad?		x		En el área de TICs regional no se hace esto.
TOTAL		1	3		

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
MATRIZ DE PONDERACIÓN**

Nº	PREGUNTAS	PONDERACIÓN	CALIFICACIÓN
1	¿La unidad de tecnología de información cuenta con un modelo de información organizacional?	10	0
2	¿El modelo de información organizacional es actualizado y documentado de forma permanente?	10	0
3	¿El modelo de información organizacional facilita la incorporación de las aplicaciones y procesos institucionales de forma transparente?	10	8
4	¿Se genera un proceso de clasificación de los datos para especificar y aplicar niveles de seguridad y propiedad?	10	5
TOTAL		40	15

DETERMINACIÓN DEL NIVEL DE RIESGO

$$CONFIANZA PONDERADA = \frac{Calificación\ Total}{Ponderación\ Total} * 100$$

$$CONFIANZA PONDERADA = \frac{15}{40} * 100$$

$$CONFIANZA PONDERADA = 37,5\%$$

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

RESULTADO:

- **CONFIANZA:** 37,5 % Bajo
- **RIESGO:** 62,5 % Alto

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

Análisis: El modelo de información organizacional facilita la incorporación de las aplicaciones y procesos institucionales de forma transparente sin embargo la unidad de TICs de la regional no está vinculada en la actualización permanente del modelo organizacional, debido a que es competencia de la unidad de comunicación existente en la matriz (Quito).

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO**

Área: TIC del IECE

Componente: Administración de proyectos tecnológicos

MOTIVO DEL EXAMEN: Conocer si la unidad de TICs define mecanismos que faciliten la administración de todos los proyectos informáticos que ejecuten en dicha unidad.

Nº	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
1	¿La unidad de tecnología de información dispone de mecanismos que faciliten la administración de todos los proyectos informáticos existentes en el área de TICs?	x			Ejecuta la matriz (no la regional)
2	¿Los proyectos tecnológicos cuentan con la descripción de la naturaleza, objetivos y alcance?	x			Ejecuta la matriz (no la regional)
3	¿Cuentan con un Cronograma de actividades que facilite la ejecución y monitoreo del proyecto?	x			Ejecuta la matriz (no la regional)
4	¿La formulación de los proyectos considerará el Costo Total de Propiedad?	x			Ejecuta la matriz (no la regional)
5	¿Para la ejecución del proyecto se define una estructura en la que se nombre un servidor responsable?	x			Ejecuta la matriz (no la regional)
6	¿Las etapas mínimas consideradas en el proyecto son: Inicio, planeación, ejecución, control, monitoreo y cierre de proyectos?	x			Ejecuta la matriz (no la regional)
7	¿Para las aprobaciones y compromisos formales se utilizan actas o documentos electrónicos legalizados?	x			Ejecuta la matriz (no la regional)
8	¿Al inicio de las etapas importantes del proyecto esté es aprobado de manera formal y comunicado a todos los interesados?	x			Ejecuta la matriz (no la regional)
9	¿Para le ejecución del proyecto se consideran un análisis de riesgos?	x			Ejecuta la matriz (no la regional)
10	¿Los riesgos identificados son permanentemente evaluados para retroalimentar el desarrollo del proyecto?	x			Ejecuta la matriz (no la regional)
11	¿Se monitorea y controla permanente los	x			Gerencia de TICs

	avances del proyecto?				Matriz
12	¿Se establece un plan de control de cambios y un plan de aseguramiento de calidad que será aprobado por las partes interesadas?	x			Gerencia de TICs Matriz
13	¿El proceso de cierre incluye la aceptación formal y pruebas que certifiquen la calidad y el cumplimiento de los objetivos planteados?	x			Unidad de TICs Proyectos Matriz
TOTAL		13	0	0	

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
MATRIZ DE PONDERACIÓN**

Nº	PREGUNTAS	PONDERACIÓN	CALIFICACIÓN
1	¿La unidad de tecnología de información dispone de mecanismos que faciliten la administración de todos los proyectos informáticos existentes en la área de TICs?	10	10
2	¿Los proyectos tecnológicos cuentan con la descripción de la naturaleza, objetivos y alcance?	10	8
3	¿Cuentan con un Cronograma de actividades que facilite la ejecución y monitoreo del proyecto?	10	8
4	¿La formulación de los proyectos considerará el Costo Total de Propiedad?	10	8
5	¿Para la ejecución del proyecto se define una estructura en la que se nombre un servidor responsable?	10	8
6	¿Las etapas mínimas consideradas en el proyecto son: Inicio, planeación, ejecución, control, monitoreo y cierre de proyectos?	10	8
7	¿Para las aprobaciones y compromisos formales se utilizan actas o documentos electrónicos legalizados?	10	8
8	¿Al inicio de las etapas importantes del proyecto esté es aprobado de manera formal y comunicado a todos los interesados?	10	8
9	¿Para le ejecución del proyecto se consideran un análisis de riesgos?	10	8
10	¿Los riesgos identificados son permanentemente evaluados para retroalimentar el desarrollo del proyecto?	10	8
11	¿Se monitorea y controla permanente los avances del proyecto?	10	8
12	¿Se establece un plan de control de cambios y un plan de aseguramiento de calidad que será aprobado por las partes interesadas?	10	8
13	¿El proceso de cierre incluye la aceptación	10	8

	formal y pruebas que certifiquen la calidad y el cumplimiento de los objetivos planteados?		
TOTAL		13	106

DETERMINACIÓN DEL NIVEL DE RIESGO

$$CONFIANZA PONDERADA = \frac{\text{Calificación Total}}{\text{Ponderación Total}} * 100$$

$$CONFIANZA PONDERADA = \frac{106}{130} * 100$$

$$CONFIANZA PONDERADA = 81,54\%$$

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

RESULTADO:

- **CONFIANZA:** Alto 81,54
- **RIESGO:** Bajo 18,46

Análisis: La unidad de TICs define mecanismos que facilitan la administración de todos los proyectos informáticos que se ejecutan en esta área, estos mecanismos se lo ejecuta en la matriz.

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO**

Área: TIC del IECE

Componente: Desarrollo y adquisición de software aplicativo

MOTIVO DEL EXAMEN: Conocer si la unidad de TICs regula los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos.

Nº	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
1	¿La adquisición de software o soluciones tecnológicas se realiza sobre la base del portafolio de proyectos y servicios priorizados en los planes estratégico y operativo?		x		Regional no realiza este proceso
2	¿Para el desarrollo y adquisición de software aplicativo se consideran aspectos como la adopción, mantenimiento y aplicación de políticas públicas y estándares internacionales?		x		Regional no realiza este proceso
3	¿La adquisición del software aplicativo se realiza en función de la identificación, priorización, especificación y acuerdos de los requerimientos funcionales y técnicos institucionales?	x			
4	¿En los procesos de desarrollo, mantenimiento o adquisición de software aplicativo se consideran estándares de desarrollo, documentación y calidad?	x			
5	¿En caso de adquisición de programas de computación (paquetes de software) estos se prevén en el proceso de compra y en los contratos respectivos?	x			
6	¿En los contratos realizados con terceros para el desarrollo de software consta que los derechos de autor son de la institución?			x	No dispone de esta información.
7	¿La implementación de software aplicativo adquirido incluye los procedimientos de configuración, aceptación y pruebas personalizadas e implantadas?	x			
8	¿Los derechos de autor del software desarrollado a la medida pertenecen a la institución?			x	No dispone de esta información.

9	¿Se elaboran manuales técnicos, de instalación y configuración?	x			
10	¿Los manuales técnicos, de instalación y configuración son difundidos, publicados y actualizados de forma permanente?	x			
TOTAL		6	2	2	

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA**

MATRIZ DE PONDERACIÓN

Nº	PREGUNTAS	PONDERACIÓN	CALIFICACIÓN
1	¿La adquisición de software o soluciones tecnológicas se realiza sobre la base del portafolio de proyectos y servicios priorizados en los planes estratégico y operativo?	10	5
2	¿Para el desarrollo y adquisición de software aplicativo se consideran aspectos como la adopción, mantenimiento y aplicación de políticas públicas y estándares internacionales?	10	5
3	¿La adquisición del software aplicativo se realiza en función de la identificación, priorización, especificación y acuerdos de los requerimientos funcionales y técnicos institucionales?	10	10
4	¿En los procesos de desarrollo, mantenimiento o adquisición de software aplicativo se consideran estándares de desarrollo, documentación y calidad?	10	8
5	¿En caso de adquisición de programas de computación (paquetes de software) estos se prevén en el proceso de compra y en los contratos respectivos?	10	8
6	¿En los contratos realizados con terceros para el desarrollo de software consta que los derechos de autor son de la institución?	10	0
7	¿La implementación de software aplicativo adquirido incluye los procedimientos de configuración, aceptación y pruebas personalizadas e implantadas?	10	8
8	¿Los derechos de autor del software	10	0

	desarrollado a la medida pertenecen a la institución?		
9	¿Se elaboran manuales técnicos, de instalación y configuración?	10	10
10	¿Los manuales técnicos, de instalación y configuración son difundidos, publicados y actualizados de forma permanente?	10	10
TOTAL		100	52

DETERMINACIÓN DEL NIVEL DE RIESGO

$$CONFIANZA PONDERADA = \frac{Calificación\ Total}{Ponderación\ Total} * 100$$

$$CONFIANZA PONDERADA = \frac{52}{100} * 100$$

$$CONFIANZA PONDERADA = 52\%$$

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

RESULTADO:

- **CONFIANZA:** 52% Moderado
- **RIESGO:** 48% Medio

Análisis: La unidad de TICs de la regional 3 no realiza la adquisición de software o soluciones tecnológicas y no dispone de información relacionada al tema, debido a que se lo realiza en la matriz de la institución, la unidad de TICs dispone de manuales técnicos de instalación y comunicación los mismos que son difundidos y publicados de forma permanente.

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO**

Área: TIC del IECE
Componente: Adquisiciones de infraestructura tecnológica

MOTIVO DEL EXAMEN: Conocer si la unidad de TICs define, justifica, implanta y actualiza la infraestructura tecnológica de la organización.

Nº	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
1	¿Las adquisiciones tecnológicas están alineadas a los objetivos de la organización y principios de calidad del servicio?	x			
2	¿Las adquisiciones tecnológicas constan en el plan anual de contrataciones aprobado de la institución?	x			
3	¿La Unidad de Tecnología de Información planifica el incremento de capacidades, evalúa los riesgos tecnológicos y los costos para futuras actualizaciones?	x			
4	¿En la adquisición de hardware en los contratos respectivos tienen el detalle suficiente que permita establecer las características técnicas de los principales componentes?	x			
5	¿En las actas de entrega/recepción se verifican los equipos adquiridos con las especificaciones técnicas y requerimientos establecidos en las fases precontractual y contractual?	x			
6	¿En los contratos con los proveedores incluyen aspectos relacionados con la seguridad y confidencialidad de la información?	x			
TOTAL		6	0	0	

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
MATRIZ DE PONDERACIÓN**

Nº	PREGUNTAS	PONDERACIÓN	CALIFICACIÓN
1	¿Las adquisiciones tecnológicas están alineadas a los objetivos de la organización y principios de calidad del servicio?	10	8
2	¿Las adquisiciones tecnológicas constan en el plan anual de contrataciones aprobado de la institución?	10	10
3	¿La Unidad de Tecnología de Información planifica el incremento de capacidades, evalúa los riesgos tecnológicos y los costos para futuras actualizaciones?	10	8
4	¿En la adquisición de hardware en los contratos respectivos tienen el detalle suficiente que permita establecer las características técnicas de los principales componentes?	10	10
5	¿En las actas de entrega/recepción se verifican los equipos adquiridos con las especificaciones técnicas y requerimientos establecidos en las fases precontractual y contractual?	10	10
6	¿En los contratos con los proveedores incluyen aspectos relacionados con la seguridad y confidencialidad de la información?	10	10
TOTAL		60	56

DETERMINACIÓN DEL NIVEL DE RIESGO

$$CONFIANZA PONDERADA = \frac{Calificación\ Total}{Ponderación\ Total} * 100$$

$$CONFIANZA PONDERADA = \frac{60}{56} * 100$$

$$CONFIANZA PONDERADA = 93,33\%$$

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

RESULTADO:

- **CONFIANZA:** 93,33% Alta
- **RIESGO:** 6,67 % Bajo

Análisis: Las adquisiciones tecnológicas están alineadas a los objetivos de la institución y constan en el plan anual de contrataciones, al momento que se recibe se verifican que los equipos adquiridos cumplan con las especificaciones técnicas y requerimientos establecidos en la fase precontractual y contractual, la unidad de TICs evalúa los riesgos tecnológicos y los costos para futuras actualizaciones.

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA**

CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO

Área: TIC del IECE

Componente: Mantenimiento y control de la infraestructura tecnológica

MOTIVO DEL EXAMEN: Conocer si la unidad de TICs define y regula los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de la entidad.

Nº	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
1	¿Se realiza una definición de procedimientos para el mantenimiento y liberación del software de aplicación?	x			
2	¿Los cambios que se realizan en los procedimientos, procesos y acuerdos de servicios son registrados, evaluados y autorizados de forma previa a su implantación?	x			
3	¿Se controla y registra las versiones del software que ingresa a la institución?	x			
4	¿Se actualizan los manuales técnicos y de usuario por cada cambio o mantenimiento que se realice?	x			
5	¿Se implementan medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos?	x			
6	¿Se elabora un plan de mantenimiento preventivo o correctivo de la infraestructura tecnológica?	x			
7	¿Se realizan revisiones periódicas y monitoreo en función de las necesidades organizacionales?	x			
8	¿Se evalúa los riesgos, vulnerabilidades y los requerimientos de seguridad?			x	Necesita reforzar esta parte.
9	¿Se mantiene el control de los bienes informáticos a través de un inventario actualizado?	x			
TOTAL		8	0	1	

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
MATRIZ DE PONDERACIÓN**

Nº	PREGUNTAS	PONDERACIÓN	CALIFICACIÓN
1	¿Se realiza una definición de procedimientos para el mantenimiento y liberación del software de aplicación?	10	8
2	¿Los cambios que se realizan en los procedimientos, procesos y acuerdos de servicios son registrados, evaluados y autorizados de forma previa a su implantación?	10	8
3	¿Se controla y registra las versiones del software que ingresa a la institución?	10	8
4	¿Se actualizan los manuales técnicos y de usuario por cada cambio o mantenimiento que se realice?	10	10
5	¿Se implementan medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos?	10	8
6	¿Se elabora un plan de mantenimiento preventivo o correctivo de la infraestructura tecnológica?	10	8
7	¿Se realizan revisiones periódicas y monitoreo en función de las necesidades organizacionales?	10	8
8	¿Se evalúa los riesgos, vulnerabilidades y los requerimientos de seguridad?	10	0
9	¿Se mantiene el control de los bienes informáticos a través de un inventario actualizado?	10	10
TOTAL		90	73

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

DETERMINACIÓN DEL NIVEL DE RIESGO

$$CONFIANZA PONDERADA = \frac{\text{Calificación Total}}{\text{Ponderación Total}} * 100$$

$$CONFIANZA PONDERADA = \frac{73}{90} * 100$$

$$CONFIANZA PONDERADA = 81,11\%$$

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

RESULTADO:

- **CONFIANZA:** Alta 81,11 %
- **RIESGO:** Bajo 18,89 %

Análisis: La unidad de TICs de la entidad cuenta de procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica; realizando revisiones periódicas y monitoreo en función de las necesidades, se mantiene un inventario actualizado de los bienes informáticos, sin embargo la definición de procedimientos para el mantenimiento y liberación del software de aplicación se lo ejecuta en la matriz, se necesita reforzar la evaluación de los riesgos, vulnerabilidades y los requerimientos de seguridad en la unidad de TICs.

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO

Área: TIC del IECE
Componente: Seguridad de tecnología de información

MOTIVO DEL EXAMEN: Conocer si la unidad de TICs establece mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

Nº	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
1	¿La unidad de tecnología de información cuenta con una ubicación adecuada?		x		Se acopla de acuerdo a lo que se tiene en la regional.
2	¿La unidad de tecnología de información dispone de un control de acceso de físico?		x		
3	¿Cuenta con procesos definidos para la obtención periódica de respaldos?	x			
4	¿En los caso de actualización de tecnologías de soporte se migra la información a los medios físicos adecuados?	x			
5	¿Se almacena respaldos con información crítica o sensible en lugares externos a la organización?	x			
6	¿Se implementa y administra seguridades a nivel de software y hardware?	x			Se necesita reforzar
7	¿Se realiza un monitoreo de seguridad al software y hardware?	x			Se necesita reforzar
8	¿Se realizan pruebas periódicas y acciones correctivas sobre las vulnerabilidades de seguridad identificados?	x			Se necesita reforzar
9	¿Existe vigilancia en el departamento de cómputo las 24 horas?		x		No existe vigilancia
10	¿Existen alarmas para detectar fuego?		x		Inexistencia de alarmas
11	¿Existen alarmas para detectar fuga de agua?		x		Inexistencia de alarmas
12	¿Existen extintores de fuego?	x			
13	¿Se ha adiestrado el personal en el manejo de		x		

	los extintores?				
14	¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?	x			
15	¿Sabén que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?	x			
16	¿Existe salida de emergencia?		x		
17	¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?	x			
18	¿Dispone el área de TICs de sitios de procesamiento alternativos?		x		
TOTAL		10	8	0	

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
MATRIZ DE PONDERACIÓN

Nº	PREGUNTAS	PONDERACIÓN	CALIFICACIÓN
1	¿La unidad de tecnología de información cuenta con una ubicación adecuada?	10	4
2	¿La unidad de tecnología de información dispone de un control de acceso de físico?	10	0
3	¿Cuenta con procesos definidos para la obtención periódica de respaldos?	10	10
4	¿En los caso de actualización de tecnologías de soporte se migra la información a los medios físicos adecuados?	10	10
5	¿Se almacena respaldos con información crítica o sensible en lugares externos a la organización?	10	10
6	¿Se implementa y administra seguridades a nivel de software y hardware?	10	8
7	¿Se realiza un monitoreo de seguridad al software y hardware?	10	8
8	¿Se realizan pruebas periódicas y acciones correctivas sobre las vulnerabilidades de seguridad identificados?	10	8
9	¿Existe vigilancia en el departamento de cómputo las 24 horas?	10	0
10	¿Existen alarmas para detectar fuego?	10	0
11	¿Existen alarmas para detectar fuga de agua?	10	0
12	¿Existen extintores de fuego?	10	10
13	¿Se ha adiestrado el personal en el manejo de los extintores?	10	0
14	¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?	10	10
15	¿Saben que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?	10	8
16	¿Existe salida de emergencia?	10	0

17	¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?	10	10
18	¿Dispone el área de TICS de sitios de procesamiento alternativos?	10	0
TOTAL		180	96

DETERMINACIÓN DEL NIVEL DE RIESGO

$$CONFIANZA PONDERADA = \frac{\text{Calificación Total}}{\text{Ponderación Total}} * 100$$

$$CONFIANZA PONDERADA = \frac{96}{180} * 100$$

$$CONFIANZA PONDERADA = 53,33\%$$

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

RESULTADO:

- **CONFIANZA:** Moderado 53,33%
- **RIESGO:** Medio 46,67%

Análisis: La unidad de TICs de la entidad cuenta con procesos definidos para la obtención periódica de respaldos, mantiene un control adecuado de la información, la unidad de TICs no cuenta con una ubicación adecuada y ha tenido que acoplarse según la disponibilidad del espacio existente, por lo que no dispone de una salida de emergencia, de alarmas para detectar fuego, ni fuga de agua, no se adiestrado al personal para el manejo adecuado de los extintores en caso de presentarse un siniestro.

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA**

CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO

Área: TIC del IECE
Componente: Plan de contingencias

MOTIVO DEL EXAMEN: Conocer si la unidad de TICs, define, aprueba e implementa un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.

N°	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
1	¿El plan de contingencias dispone de un plan de respuesta a los riesgos?		x		
2	¿El plan de contingencias cuenta con procedimientos de control de cambios?	x			
3	¿El plan de contingencias cuenta con un plan de continuidad de las operaciones?	x			
4	¿El plan de contingencias cuenta con un plan de recuperación de desastres?		x		
5	¿Se ha designado un comité con nombres y roles específico para ejecutar las funciones de contingencia en caso de suscitarse una emergencia?		x		
6	¿La aplicación del plan permite recuperar la operación de los sistemas en un nivel aceptable?	x			
7	¿La aplicación del plan permitirá salvaguardar la integridad y seguridad de la información?	x			
8	¿El plan de contingencias aprobado, es difundido entre el personal responsable de su ejecución?		x		
9	¿El plan de contingencias es sometido a pruebas, entrenamientos y evaluaciones periódicas?		x		
TOTAL		4	5		

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
MATRIZ DE PONDERACIÓN**

Nº	PREGUNTAS	PONDERACIÓN	CALIFICACIÓN
1	¿El plan de contingencias dispone de un plan de respuesta a los riesgos?	10	0
2	¿El plan de contingencias cuenta con procedimientos de control de cambios?	10	10
3	¿El plan de contingencias cuenta con un plan de continuidad de las operaciones?	10	10
4	¿El plan de contingencias cuenta con un plan de recuperación de desastres?	10	0
5	¿Se ha designado un comité con nombres y roles específicos para ejecutar las funciones de contingencia en caso de suscitarse una emergencia?	10	0
6	¿La aplicación del plan permite recuperar la operación de los sistemas en un nivel aceptable?	10	8
7	¿La aplicación del plan permitirá salvaguardar la integridad y seguridad de la información?	10	8
8	¿El plan de contingencias aprobado, es difundido entre el personal responsable de su ejecución?	10	0
9	¿El plan de contingencias es sometido a pruebas, entrenamientos y evaluaciones periódicas?	10	0
TOTAL		90	36

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

DETERMINACIÓN DEL NIVEL DE RIESGO

$$CONFIANZA PONDERADA = \frac{\text{Calificación Total}}{\text{Ponderación Total}} * 100$$

$$CONFIANZA PONDERADA = \frac{36}{90} * 100$$

$$CONFIANZA PONDERADA = 40\%$$

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

RESULTADO:

- **CONFIANZA:** Bajo 40%
- **RIESGO:** Alto 60%

Análisis: Como se puede observar el riesgo obtenido en la evaluación del plan de contingencias es alto con un 60% debido a que no dispone de un plan de respuesta a los riesgos, no cuenta con un plan de recuperación de desastres, no se ha designado un comité con nombres y roles específicos para ejecutar las funciones de contingencia en caso de suscitarse una emergencia, no es aprobado ni difundido entre el personal responsable de su ejecución y no se ha sometido a pruebas, entrenamiento y evaluaciones periódicas.

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO**

Área: TIC del IECE

Componente: Administración de soporte de tecnología de información

MOTIVO DEL EXAMEN: Conocer si la unidad de TICs, define, aprueba y difunde procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garantice la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos.

Nº	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
1	¿Se realizan revisiones periódicas para determinar si la capacidad y desempeño actual y futuro de los recursos tecnológicos son suficientes para cubrir los niveles de servicio acordados con los usuarios?		x		
2	¿Se mantiene una seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales de la entidad?	x			
3	¿Se ha estandarizado la identificación, autenticación y autorización de los usuarios y administración de sus cuentas?	x			
4	¿Se realizan revisiones regulares de todas las cuentas de usuarios?	x			
5	¿Existen medidas de prevención, detección y corrección que protejan a los sistemas de información y a la tecnología de la organización de software malicioso y virus informáticos?	x			
6	¿Los procesos críticos de tecnología de información en el manejo de niveles de servicio y operación son manejados adecuadamente?	x			
7	¿Se realiza una alineación de los servicios claves de tecnología de información con los requerimientos y las prioridades de la organización?	x			
8	¿Se administra los incidentes reportados, requerimientos de servicio y solicitudes de información y de cambios que demandan los usuarios?	x			
9	¿Se mantiene un repositorio de diagramas y configuraciones de hardware y software	x			

	actualizado?				
10	¿Se administra adecuadamente la información?	x			
11	¿Se administra adecuadamente los respaldos y recuperación de datos?	x			
12	¿Se han incorporado mecanismos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información?	x			
TOTAL		11	1	0	

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
MATRIZ DE PONDERACIÓN

Nº	PREGUNTAS	PONDERACIÓN	CALIFICACIÓN
1	¿Se realizan revisiones periódicas para determinar si la capacidad y desempeño actual y futuro de los recursos tecnológicos son suficientes para cubrir los niveles de servicio acordados con los usuarios?	10	0
2	¿Se mantiene una seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales de la entidad?	10	10
3	¿Se ha estandarizado la identificación, autenticación y autorización de los usuarios y administración de sus cuentas?	10	10
4	¿Se realizan revisiones regulares de todas las cuentas de usuarios?	10	8
5	¿Existen medidas de prevención, detección y corrección que protejan a los sistemas de información y a la tecnología de la organización de software malicioso y virus informáticos?	10	10
6	¿Los procesos críticos de tecnología de información en el manejo de niveles de servicio y operación son manejados adecuadamente?	10	8
7	¿Se realiza una alineación de los servicios claves de tecnología de información con los requerimientos y las prioridades de la organización?	10	8
8	¿Se administra los incidentes reportados, requerimientos de servicio y solicitudes de información y de cambios que demandan los usuarios?	10	8
9	¿Se mantiene un repositorio de diagramas y configuraciones de hardware y software actualizado?	10	10
10	¿Se administra adecuadamente la información?	10	10
11	¿Se administra adecuadamente los respaldos y recuperación de datos?	10	10

12	¿Se han incorporado mecanismos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información?	10	8
TOTAL		120	100

DETERMINACIÓN DEL NIVEL DE RIESGO

$$CONFIANZA PONDERADA = \frac{\text{Calificación Total}}{\text{Ponderación Total}} * 100$$

$$CONFIANZA PONDERADA = \frac{100}{120} * 100$$

$$CONFIANZA PONDERADA = 83,33\%$$

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

RESULTADO:

- **CONFIANZA:** Alta 83,33 %
- **RIESGO:** Bajo 16,67%

Análisis: En la unidad de TICs la administración de soporte de tecnología de información es manejada de manera adecuada; se mantiene una seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales de la entidad, se realizan revisiones regulares de todas las cuentas de usuarios, existen medidas de prevención, detección y corrección que protejan a los sistemas de información y a la tecnología de la organización de software maliciosos y virus informáticos, la debilidad encontrada es que no se realizan revisiones periódicas para determinar si la capacidad y desempeño actual y futuro de los recursos tecnológicos son suficientes para cubrir los niveles de servicio acordados con los usuarios.

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO**

Área: TIC del IECE

Componente: Monitoreo y evaluación de los procesos y servicios

MOTIVO DEL EXAMEN: Conocer si la entidad cuenta con un marco de trabajo de monitoreo y definición del alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad.

Nº	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
1	¿Se ha establecido un marco de trabajo de monitoreo para los procesos y servicios?	x			
2	¿Se define el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad?		x		
3	¿Se han definido indicadores de desempeño y métricas del proceso para monitorear la gestión?	x			Falta reforzar
4	¿La Unidad de Tecnología de Información define y ejecuta procedimientos para la medición, análisis y mejora del nivel de satisfacción de los clientes internos y externos por los servicios recibidos?	x			Falta reforzar
5	¿La Unidad de Tecnología de Información presenta informes periódicos de gestión a la alta dirección, para que ésta supervise el cumplimiento de los objetivos planteados?	x			
TOTAL		4	1	0	

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
MATRIZ DE PONDERACIÓN**

Nº	PREGUNTAS	PONDERACIÓN	CALIFICACIÓN
1	¿Se ha establecido un marco de trabajo de monitoreo para los procesos y servicios?	10	10
2	¿Se define el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad?	10	0
3	¿Se han definido indicadores de desempeño y métricas del proceso para monitorear la gestión?	10	8
4	¿La Unidad de Tecnología de Información define y ejecuta procedimientos para la medición, análisis y mejora del nivel de satisfacción de los clientes internos y externos por los servicios recibidos?	10	8
5	¿La Unidad de Tecnología de Información presenta informes periódicos de gestión a la alta dirección, para que ésta supervise el cumplimiento de los objetivos planteados?	10	8
TOTAL		50	34

DETERMINACIÓN DEL NIVEL DE RIESGO

$$CONFIANZA PONDERADA = \frac{Calificación\ Total}{Ponderación\ Total} * 100$$

$$CONFIANZA PONDERADA = \frac{34}{50} * 100$$

$$CONFIANZA PONDERADA = 68\%$$

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

RESULTADO:

- **CONFIANZA:** Moderado 68%
- **RIESGO:** Medio 32%

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

Análisis: En la unidad de TICs se ha establecido un marco de trabajo de monitoreo para los procesos y servicios, se presentan informes periódicos de la gestión a la alta dirección (se cuenta con software que registra los requerimientos y soportes atendidos), sin embargo falta reforzar en ciertos aspectos como en la definición y ejecución de procedimientos para la medición, análisis y mejora del nivel de satisfacción de los clientes internos y externos por los servicios recibidos, y no se define el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad.

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO**

Área: TIC del IECE

Componente: Sitio web, servicios de internet e intranet

MOTIVO DEL EXAMEN: Conocer si la unidad de TICs elabora las normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio web de la entidad, a base de las disposiciones legales y normativas y los requerimientos de los usuarios externos e internos.

Nº	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
1	¿La Unidad de Tecnología de Información elabora normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio web de la entidad?	x			
2	¿Las normas, procedimientos e instructivos se realizan en base a las disposiciones legales y normativas?	x			
3	¿Las normas, procedimientos e instructivos se realizan en base a los requerimientos de los usuarios externos e internos?	x			
4	¿La Unidad de Tecnología de Información considera el desarrollo de aplicaciones web y/o móviles que automaticen los procesos o trámites orientados al uso de instituciones y ciudadanos en general?	x			
TOTAL		4	0	0	

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
MATRIZ DE PONDERACIÓN**

Nº	PREGUNTAS	PONDERACIÓN	CALIFICACIÓN
1	¿La Unidad de Tecnología de Información elabora normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio web de la entidad?	10	10
2	¿Las normas, procedimientos e instructivos se realizan en base a las disposiciones legales y normativas?	10	10
3	¿Las normas, procedimientos e instructivos se realizan en base a los requerimientos de los usuarios externos e internos?	10	8
4	¿La Unidad de Tecnología de Información considera el desarrollo de aplicaciones web y/o móviles que automaticen los procesos o trámites orientados al uso de instituciones y ciudadanos en general?	10	8
TOTAL		40	36

DETERMINACIÓN DEL NIVEL DE RIESGO

$$CONFIANZA PONDERADA = \frac{Calificación\ Total}{Ponderación\ Total} * 100$$

$$CONFIANZA PONDERADA = \frac{36}{40} * 100$$

$$CONFIANZA PONDERADA = 90 \%$$

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

RESULTADO:

- **CONFIANZA:** Alta 90%
- **RIESGO:** Bajo 10%

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

Análisis: La unidad de TICs elabora normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio web de la entidad, a base de las disposiciones legales, normativas y los requerimientos de los usuarios externos e internos.

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA**

CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO

Área: TIC del IECE
Componente: Capacitación Informática

MOTIVO DEL EXAMEN: Conocer si la entidad identifica las necesidades de capacitación tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información.

Nº	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
1	¿Cuenta la entidad con un plan de capacitación informático?	x			
2	¿Las necesidades de capacitación son identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información?	x			
3	¿El plan de capacitación informático esta formulado conjuntamente con la Unidad de Talento Humano?	x			
4	¿El plan de capacitación informático está orientado a los puestos de trabajo?	x			
5	¿El plan de capacitación informático está orientado a las necesidades de conocimiento específicas determinadas en la evaluación de desempeño e institucionales?	x			
TOTAL		5	0	0	

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
MATRIZ DE PONDERACIÓN**

Nº	PREGUNTAS	PONDERACIÓN	CALIFICACIÓN
1	¿Cuenta la entidad con un plan de capacitación informático?	10	10
2	¿Las necesidades de capacitación son identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información?	10	10
3	¿El plan de capacitación informático esta formulado conjuntamente con la Unidad de Talento Humano?	10	10
4	¿El plan de capacitación informático está orientado a los puestos de trabajo?	10	10
5	¿El plan de capacitación informático está orientado a las necesidades de conocimiento específicas determinadas en la evaluación de desempeño e institucionales?	10	6
TOTAL		50	46

DETERMINACIÓN DEL NIVEL DE RIESGO

$$CONFIANZA PONDERADA = \frac{Calificación\ Total}{Ponderación\ Total} * 100$$

$$CONFIANZA PONDERADA = \frac{46}{50} * 100$$

$$CONFIANZA PONDERADA = 92\%$$

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

RESULTADO:

- **CONFIANZA:** Alta 92%
- **RIESGO:** Bajo 8%

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

Análisis: En la entidad se identifica las necesidades de capacitación tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, sin embargo falta reforzar que el plan de capacitación informático este orientado a las necesidades de conocimiento específicas, determinadas en la evaluación de desempeño.

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO**

Área: TIC del IECE
Componente: Comité Informático

MOTIVO DEL EXAMEN: Conocer si la entidad cuenta con un comité informático.

Nº	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
1	¿Dispone la entidad de un comité informático?	x			
2	¿El comité informático tiene definido claramente los objetivos que persigue?	x			
3	¿El propósito fundamental del comité informático es definir, conducir y evaluar las políticas internas para el crecimiento ordenado y progresivo de la tecnología de la información y la calidad de los servicios informáticos?	x			
4	¿El comité informático apoya en esta materia a las unidades administrativas que conforman la entidad?	x			
TOTAL		4	0	0	

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
MATRIZ DE PONDERACIÓN**

Nº	PREGUNTAS	PONDERACIÓN	CALIFICACIÓN
1	¿Dispone la entidad de un comité informático?	10	10
2	¿El comité informático tiene definido claramente los objetivos que persigue?	10	10
3	¿El propósito fundamental del comité informático es definir, conducir y evaluar las políticas internas para el crecimiento ordenado y progresivo de la tecnología de la información y la calidad de los servicios informáticos?	10	8
4	¿El comité informático apoya en esta materia a las unidades administrativas que conforman la entidad?	10	8
TOTAL		40	36

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

DETERMINACIÓN DEL NIVEL DE RIESGO

$$CONFIANZA PONDERADA = \frac{\text{Calificación Total}}{\text{Ponderación Total}} * 100$$

$$CONFIANZA PONDERADA = \frac{36}{40} * 100$$

$$CONFIANZA PONDERADA = 90 \%$$

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

RESULTADO:

- **CONFIANZA:** Alto 90%
- **RIESGO:** Bajo 10%

Análisis: La entidad dispone de un comité informático, el cual tiene claramente definido los objetivos que persigue, cumpliendo con el propósito fundamental que es definir, conducir y evaluar las políticas internas para el crecimiento ordenado y progresivo de la tecnología de información.

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA**

CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO

Área: TIC del IECE
Componente: Firmas electrónicas

MOTIVO DEL EXAMEN: Conocer si la entidad ajusta sus procedimientos, operaciones e incorporación de medios técnicos necesarios, para permitir el uso de la firma electrónica de conformidad con la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su reglamento.

Nº	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
1	¿La entidad utiliza una firma electrónica para ejecutar sus operaciones?	x			
2	¿La entidad ajusta sus procedimientos y operaciones e incorpora los medios técnicos necesarios, para permitir el uso de la firma electrónica?	x			
3	¿Se verifica mediante procesos automatizados de validación, que el certificado de la firma electrónica recibida es emitido por una entidad de certificación de información acreditada?		x		
4	¿Se verifica que el certificado de la firma electrónica recibida se encuentre vigente?	x			
5	¿Se coordina y define los formatos y tipos de archivo digitales en el uso de la firma electrónica?		x		
6	¿Los archivos electrónicos o mensajes de datos firmados electrónicamente se conservan en su estado original en medios electrónicos seguros?	x			
7	¿Los archivos electrónicos o mensajes de datos firmados electrónicamente son conservados por el usuario que los generó?	x			
8	¿Cuenta la entidad con políticas internas de manejo y archivo de información digital?		x		
9	¿Se notifica a la entidad de certificación de información sobre cualquier cambio, modificación o variación de los datos?		x		
10	¿Los titulares de certificados de firma electrónica y dispositivos portables seguros	x			

	son responsables de su buen uso y protección?				
11	¿Las claves de acceso son divulgadas y compartidas?		x		
12	¿Se solicita la revocación del certificado de firma electrónica cuando se presenta cualquier circunstancia que pueda comprometer su utilización?		x		
13	¿Se solicita la renovación del certificado de firma electrónica con la debida anticipación?	x			
14	¿La entidad de certificación capacita e informa a los solicitantes respecto de las medidas de seguridad y responsabilidades que deben observar en el uso de los servicios contratados?	x			
15	¿Esta capacitación facilita la comprensión y utilización de las firmas electrónicas?	x			
TOTAL		9	6	0	

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
MATRIZ DE PONDERACIÓN

Nº	PREGUNTAS	PONDERACIÓN	CALIFICACIÓN
1	¿La entidad utiliza una firma electrónica para ejecutar sus operaciones?	10	8
2	¿La entidad ajusta sus procedimientos y operaciones e incorpora los medios técnicos necesarios, para permitir el uso de la firma electrónica?	10	10
3	¿Se verifica mediante procesos automatizados de validación, que el certificado de la firma electrónica recibida es emitido por una entidad de certificación de información acreditada?	10	0
4	¿Se verifica que el certificado de la firma electrónica recibida se encuentre vigente?	10	10
5	¿Se coordina y define los formatos y tipos de archivo digitales en el uso de la firma electrónica?	10	0
6	¿Los archivos electrónicos o mensajes de datos firmados electrónicamente se conservan en su estado original en medios electrónicos seguros?	10	10
7	¿Los archivos electrónicos o mensajes de datos firmados electrónicamente son conservados por el usuario que los generó?	10	10
8	¿Cuenta la entidad con políticas internas de manejo y archivo de información digital?	10	0
9	¿Se notifica a la entidad de certificación de información sobre cualquier cambio, modificación o variación de los datos?	10	0
10	¿Los titulares de certificados de firma electrónica y dispositivos portables seguros son responsables de su buen uso y protección?	10	10
11	¿Las claves de acceso son divulgadas y compartidas?	10	10
12	¿Se solicita la revocación del certificado de firma electrónica cuando se presenta cualquier circunstancia que pueda comprometer su utilización?	10	0

13	¿Se solicita la renovación del certificado de firma electrónica con la debida anticipación?	10	10
14	¿La entidad de certificación capacita e informa a los solicitantes respecto de las medidas de seguridad y responsabilidades que deben observar en el uso de los servicios contratados?	10	8
15	¿Esta capacitación facilita la comprensión y utilización de las firmas electrónicas?	10	8
TOTAL		150	94

DETERMINACIÓN DEL NIVEL DE RIESGO

$$CONFIANZA PONDERADA = \frac{\text{Calificación Total}}{\text{Ponderación Total}} * 100$$

$$CONFIANZA PONDERADA = \frac{94}{150} * 100$$

$$CONFIANZA PONDERADA = 62,67\%$$

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

RESULTADO:

- **CONFIANZA:** Moderado 62,67 %
- **RIESGO:** Medio 37,33%

Análisis: La gerencia regional es la única que utiliza una firma electrónica para ejecutar sus actividades, la entidad ajusta sus procedimientos y operaciones e incorpora los medios técnicos necesarios, para permitir el uso de la firma electrónica a través del sistema quipux, se verifica que el certificado de la firma electrónica recibida se encuentre vigente, los archivos electrónicos o mensajes de datos firmados electrónicamente se conservan en su estado original en medios electrónicos seguros, las claves de acceso se mantienen en secreto y no son divulgadas, sin embargo la entidad no cuenta con políticas internas de manejo y archivo de información digital, no se verifica mediante procesos automatizados de validación, que el certificado de la firma electrónica recibida es emitido por una entidad de certificación de información acreditada y no se coordina y define los formatos y tipos de archivo digitales en el uso de la firma electrónica.

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO**

Área: TIC del IECE

Componente: Controles sobre sistemas de información

MOTIVO DEL EXAMEN: Conocer si los sistemas de información cuentan con controles adecuados para garantizar confiabilidad, seguridad y una clara administración de los niveles de acceso a la información y datos sensibles.

Nº	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
1	¿El sistema de información permite a la máxima autoridad evaluar los resultados de la gestión en la entidad?	x			
2	¿Los sistemas de información y comunicación que se diseñan e implantan concuerdan con los planes estratégicos y operativos?	x			
3	¿Los sistemas de información están constituidos por métodos establecidos para registrar, procesar, resumir e informar sobre las operaciones administrativas y financieras de la entidad?	x			
4	¿Los sistemas de información mantienen controles apropiados?	x			
5	¿Los sistemas automatizados cuentan con controles generales, de aplicación y de operación que garanticen la protección de la información?	x			
6	¿Los sistemas automatizados permiten obtener con disponibilidad, accesibilidad y oportunidad la información?	x			
7	¿Se establecen controles pertinentes para que garanticen razonablemente la calidad de la información y de la comunicación?	x			
TOTAL		7	0	0	

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
MATRIZ DE PONDERACIÓN**

Nº	PREGUNTAS	PONDERACIÓN	CALIFICACIÓN
1	¿El sistema de información permite a la máxima autoridad evaluar los resultados de la gestión en la entidad?	10	9
2	¿Los sistemas de información y comunicación que se diseñan e implantan concuerdan con los planes estratégicos y operativos?	10	10
3	¿Los sistemas de información están constituidos por métodos establecidos para registrar, procesar, resumir e informar sobre las operaciones administrativas y financieras de la entidad?	10	10
4	¿Los sistemas de información mantienen controles apropiados?	10	9
5	¿Los sistemas automatizados cuentan con controles generales, de aplicación y de operación que garanticen la protección de la información?	10	8
6	¿Los sistemas automatizados permiten obtener con disponibilidad, accesibilidad y oportunidad la información?	10	9
7	¿Se establecen controles pertinentes para que garanticen razonablemente la calidad de la información y de la comunicación?	10	9
TOTAL		70	63

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

DETERMINACIÓN DEL NIVEL DE RIESGO

$$CONFIANZA PONDERADA = \frac{\text{Calificación Total}}{\text{Ponderación Total}} * 100$$

$$CONFIANZA PONDERADA = \frac{63}{70} * 100$$

$$CONFIANZA PONDERADA = 90\%$$

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

RESULTADO:

- **CONFIANZA:** Alto 90%
- **RIESGO:** Bajo 10%

Análisis: Los sistemas de información cuentan con controles adecuados para garantizar confiabilidad, seguridad y una clara administración de los niveles de acceso a la información y datos sensibles en la entidad.

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO**

Área: TIC del IECE
Componente: Canales de comunicación abiertos

MOTIVO DEL EXAMEN: Conocer si se establecerán canales de comunicación abiertos, que permitan trasladar la información de manera segura, correcta y oportuna a los destinatarios dentro y fuera de la institución.

Nº	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
1	¿Se establece en la entidad canales de comunicación abiertos?	x			
2	¿Los canales de comunicación abiertos permiten trasladar la información de manera segura, correcta y oportuna a los destinatarios dentro y fuera de la institución?	x			
3	¿La comunicación interna permitir interacciones entre las servidoras y servidores?	x			
4	¿La comunicación interna permitir interacciones entre las distintas unidades administrativas de la institución?	x			
5	¿La entidad dispone de canales abiertos de comunicación que permita a los usuarios aportar información de gran valor sobre el diseño y la calidad de los productos y servicios brindados?	x			
TOTAL		5	0	0	

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - REGIONAL 3
RIOBAMBA
MATRIZ DE PONDERACIÓN**

Nº	PREGUNTAS	PONDERACIÓN	CALIFICACIÓN
1	¿Se establece en la entidad canales de comunicación abiertos?	10	10
2	¿Los canales de comunicación abiertos permiten trasladar la información de manera segura, correcta y oportuna a los destinatarios dentro y fuera de la institución?	10	8
3	¿La comunicación interna permitir interacciones entre las servidoras y servidores?	10	8
4	¿La comunicación interna permitir interacciones entre las distintas unidades administrativas de la institución?	10	8
5	¿La entidad dispone de canales abiertos de comunicación que permita a los usuarios aportar información de gran valor sobre el diseño y la calidad de los productos y servicios brindados?	10	8
TOTAL		50	42

DETERMINACIÓN DEL NIVEL DE RIESGO

$$CONFIANZA PONDERADA = \frac{Calificación\ Total}{Ponderación\ Total} * 100$$

$$CONFIANZA PONDERADA = \frac{42}{50} * 100$$

$$CONFIANZA PONDERADA = 84 \%$$

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

RESULTADO:

- **CONFIANZA:** Alto 84%
- **RIESGO:** Bajo 16%

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

Análisis: En la entidad se establecen canales de comunicación abiertos, que permitan trasladar la información de manera segura, correcta y oportuna a los destinatarios dentro y fuera de la institución sin embargo falta reforzar que la comunicación interna permita interacciones entre las servidoras y servidores en las distintas unidades administrativas de la institución.

REALIZADO POR: AMOY	FECHA: 27-07-2013
REVISADO POR: BNCO	FECHA: 17-08-2013

PLANIFICACIÓN DEL MANTENIMIENTO DE EQUIPOS.

El mantenimiento preventivo de los equipos informáticos en la regional se lo realiza dos veces al año según lo señalado en Plan operativo anual (POA) sin embargo, el mantenimiento correctivo se procede de acuerdo a las necesidades institucionales según se presente el caso.

RESULTADO ESPERADO	ACTIVIDADES	META PROGRAMADA	CRONOGRAMA												RESPONSABLE	PRESUPUESTO	DPTO. RESPONSABLE	INDICADOR	% CUMPLIMIENTO	OBSERVACIONES		
		INDICADORES	MESES																			
			e	f	m	a	m	j	j	a	s	o	n	d								
21.Programa para el mejoramiento y mantenimiento del Paquete Tecnológico de la Regional	21.1 Identificación de Problemas y Causas en la Aplicación del Sistema Operativo SIGEN	Al 30 de cada mes se tendrá un reporte de los problemas tecnológicos existentes	x	x	x	x	x	x	x	x	x	x	x	x	x		Informática Matriz e Informático Regional	Recursos Humanos	Sistemas	No. De reportes con problemas tecnológicos realizados en el mes/No. De reportes con problemas tecnológicos programados en el mes	100%	
	21.2 Análisis y desarrollo de soluciones a Problemas Identificados	Comunicación permanente los 365 días del año 2012 con los funcionarios de Sistemas Matriz para la solución constante	x	x	x	x	x	x	x	x	x	x	x	x	x		Informática Matriz e Informático Regional					100%

REALIZADO POR: AMOY	FECHA: 09-08-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

<p>21.3 Pruebas e Implementación de soluciones</p>	<p>Diariamente los funcionarios encargados del programa institucional que presenta problemas, harán las pruebas respectivas de las soluciones otorgadas por la Matriz en un 100%</p>	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	<p>Informática Matriz e Informático Regional</p>					
<p>21.4 Desarrollo e Implementación de Tecnologías de Información. (Procesos de Secretaría, Seguimiento Académico, Seguimiento Situación Económica Deudores y Garantes, Archivo, Atención al Cliente, Becas)</p>	<p>Se aplicarán todos los cambios y modalidades operativas que la matriz desarrolle en beneficio de la institución en un 100% los 365 días del año</p>	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	<p>Informática Matriz e Informático Regional</p>	<p>Recursos Humanos</p>	<p>Sistemas</p>			

<p>REALIZADO POR:</p>	<p>FECHA:</p>
<p>AMOY</p>	<p>09-08-2013</p>
<p>REVISADO POR:</p>	<p>FECHA:</p>
<p>BNCO</p>	<p>18-12-2013</p>

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS (IECE) REGIONAL 3 RIOBAMBA
VERIFICACIÓN DE MEDIDAS DE SEGURIDAD**

CARACTERÍSTICAS	DETALLE	CUMPLE		OBSERVACIÓN
		SI	NO	
Los accesos	Existe acceso adecuado al área de TICs	✓		
	Las puertas del área de TICs son amplias.		✓	
La seguridad	Existe circuito cerrado de cámaras en la entidad		✓	
	Existe una persona encargada de la seguridad "guardia que custodie los bienes del área de TICs	✓		
	El área de TICs está en un lugar seguro	✓		
	Posee puertas metálicas de protección		✓	
	Existe salida de emergencia		✓	
	Existen extintores de incendios en la área	✓		
	Posee alarma		✓	
	Existe un mecanismo de control de ingreso al área de TICs		✓	
El cableado	El cableado del área de TICs se encuentra oculto	✓		
	Existe UPS, que solventa perdida de energia	✓		
Otros	Existe un sitio adecuado para el mantenimiento de los equipos	✓		
	Existe mantenimiento programado por escrito de forma permanente	✓		
	El área de TICs cuenta con una empresa aseguradora	✓		

REALIZADO POR: AMOY	FECHA: 13-08-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

**INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS (IECE)
REGIONAL 3 RIOBAMBA
CONDICIONES DEL ÁREA DE TICS**

CARACTERÍSTICAS	DETALLE	CUMPLE		OBSERVACIÓN
		SI	NO	
UNIDAD ADMINISTRATIVA Y FINANCIERA				
Iluminación	Funciona todos los puntos de iluminación	✓		
	Independencia de interruptores eléctricos	✓		
	Adecuado nivel de luz eléctrica	✓		
Temperatura	Existe un sistema de ventilación que mantenga una temperatura adecuada		✓	
	Ingresar polvo por las ventanas		✓	
	Afecta a los usuarios la temperatura	✓		
	Afecta a los equipos la alta temperatura		✓	
Otros elementos	Funcionamiento adecuado de la impresora	✓		
	Distribución física adecuada	✓		
	Aseo	✓		
UNIDAD COACTIVAS				
Iluminación	Funciona todos los puntos de iluminación	✓		
	Independencia de interruptores eléctricos	✓		
	Adecuado nivel de luz eléctrica	✓		
Temperatura	Existe un sistema de ventilación que mantenga una temperatura adecuada		✓	
	Ingresar polvo por las ventanas		✓	
	Afecta a los usuarios la temperatura		✓	
	Afecta a los equipos la alta temperatura		✓	
Otros elementos	Funcionamiento adecuado de la impresora	✓		
	Distribución física adecuada	✓		
	Aseo	✓		
UNIDAD DE CRÉDITO				
Iluminación	Funciona todos los puntos de iluminación	✓		
	Independencia de interruptores eléctricos	✓		
	Adecuado nivel de luz eléctrica	✓		
Temperatura	Existe un sistema de ventilación que mantenga una temperatura adecuada		✓	
	Ingresar polvo por las ventanas		✓	
	Afecta a los usuarios la temperatura		✓	
	Afecta a los equipos la alta temperatura		✓	
Otros elementos	Funcionamiento adecuado de la impresora	✓		
	Distribución física adecuada	✓		
	Aseo	✓		
UNIDAD DE BECAS				
Iluminación	Funciona todos los puntos de iluminación	✓		
	Independencia de interruptores eléctricos	✓		
	Adecuado nivel de luz eléctrica	✓		
Temperatura	Existe un sistema de ventilación que mantenga una temperatura adecuada		✓	
	Ingresar polvo por las ventanas		✓	

REALIZADO POR: AMOY	FECHA: 16-08-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

	Afecta a los usuarios la temperatura		✓	
	Afecta a los equipos la alta temperatura		✓	
Otros elementos	Funcionamiento adecuado de la impresora	✓		
	Distribución física adecuada	✓		
	Aseo	✓		
UNIDAD DE TICS				
Iluminación	Funciona todos los puntos de iluminación	✓		
	Independencia de interruptores eléctricos	✓		
	Adecuado nivel de luz eléctrica	✓		
Temperatura	Existe un sistema de ventilación que mantenga una temperatura adecuada		✓	
	Ingresar polvo por las ventanas	✓		
	Afecta a los usuarios la temperatura		✓	
	Afecta a los equipos la alta temperatura		✓	
Otros elementos	Funcionamiento adecuado de la impresora	✓		
	Distribución física adecuada	✓		
	Aseo	✓		

REALIZADO POR: AMOY	FECHA: 16-08-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS (IECE) REGIONAL 3 RIOBAMBA
VERIFICACIÓN DE CAMBIO DE CONTRASEÑAS A LOS SISTEMAS DE INFORMACIÓN

Objetivo: verificar si se establecen cambios de claves de acceso a los sistemas de información durante un determinado periodo de tiempo por parte del personal de la entidad.

											OBSERVACIONES	
Usuario	Se tienen establecido políticas de cambio de claves de acceso a los usuarios de los sistemas de información como sistema de la entidad, correos electrónicos etc.	SI	✓	Cada qué periodo de tiempo lo realiza	30 días	Las contraseñas que mantiene para el ingreso a los sistemas de información, principalmente sistema de la entidad y correo electrónico se considera un sistema de seguridad:	Alta	✓	El sistema de la entidad permite que las claves de acceso tengan un determinado tiempo de caducidad y por lo tanto notificar al usuario que se debe realizar cambios	SI	✓	
Funcionarios Unidad Adm. Finanzas		NO			60 días		Media			NO		
					180 días							Baja
					Anual							
Nunca												
Usuario	Se tienen establecido políticas de cambio de claves de acceso a los usuarios de los sistemas de información como sistema de la entidad, correos electrónicos etc.	SI	✓	Cada qué periodo de tiempo lo realiza	30 días	Las contraseñas que mantiene para el ingreso a los sistemas de información, principalmente sistema de la entidad y correo electrónico se considera un sistema de seguridad:	Alta	✓	El sistema de la entidad permite que las claves de acceso tengan un determinado tiempo de caducidad y por lo tanto notificar al usuario que se debe realizar cambios	SI	✓	
Funcionarios Unidad Adm. Finanzas		NO			60 días		Media			NO		
					180 días							Baja
					Anual							
Nunca												
Usuario	Se tienen establecido políticas de cambio de claves de acceso a los usuarios de los sistemas de información como sistema de la entidad, correos electrónicos etc.	SI	✓	Cada qué periodo de tiempo lo realiza	30 días	Las contraseñas que mantiene para el ingreso a los sistemas de información, principalmente sistema de la entidad y correo electrónico se considera un sistema de seguridad:	Alta	✓	El sistema de la entidad permite que las claves de acceso tengan un determinado tiempo de caducidad y por lo tanto notificar al usuario que se debe realizar cambios	SI	✓	
Funcionarios Unidad Administrativa		NO			60 días		Media			NO		
					180 días							Baja
					Anual							
Nunca												
Usuario	Se tienen establecido políticas de cambio de claves de acceso a los usuarios de los sistemas de información como sistema de la entidad, correos electrónicos etc.	SI	✓	Cada qué periodo de tiempo lo realiza	30 días	Las contraseñas que mantiene para el ingreso a los sistemas de información, principalmente sistema de la entidad y correo electrónico se considera un sistema de seguridad:	Alta	✓	El sistema de la entidad permite que las claves de acceso tengan un determinado tiempo de caducidad y por lo tanto notificar al usuario que se debe realizar cambios	SI	✓	
Funcionarios Coactivos		NO			60 días		Media			NO		
					180 días							Baja
					Anual							
Nunca												
Usuario	Se tienen establecido políticas de cambio de claves de acceso a los usuarios de los sistemas de información como sistema de la entidad, correos electrónicos etc.	SI	✓	Cada qué periodo de tiempo lo realiza	30 días	Las contraseñas que mantiene para el ingreso a los sistemas de información, principalmente sistema de la entidad y correo electrónico se considera un sistema de seguridad:	Alta	✓	El sistema de la entidad permite que las claves de acceso tengan un determinado tiempo de caducidad y por lo tanto notificar al usuario que se debe realizar cambios	SI	✓	
Funcionarios Crédito		NO			60 días		Media			NO		
					180 días							Baja
					Anual							
Nunca												

REALIZADO POR: AMOY	FECHA: 23-08-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS (IECE) REGIONAL 3 RIOBAMBA
VERIFICACIÓN DE CAMBIO DE CONTRASEÑAS A LOS SISTEMAS DE INFORMACIÓN

Objetivo: verificar si se establecen cambios de claves de acceso a los sistemas de información durante un determinado periodo de tiempo por parte del personal de la entidad.

											OBSERVACIONES				
Usuario	Se tienen establecido políticas de cambio de claves de acceso a los usuarios de los sistemas de información como sistema de la entidad, correos electrónicos etc.	SI	✓	Cada qué periodo de tiempo lo realiza	30 días		Las contraseñas que mantiene para el ingreso a los sistemas de información, principalmente sistema de la entidad y correo electrónico se considera un sistema de seguridad:	Alta	✓	El sistema de la entidad permite que las claves de acceso tengan un determinado tiempo de caducidad y por lo tanto notificar al usuario que se debe realizar cambios	SI	✓			
					60 días	✓			Media						
Funcionario Credito		NO				180 días					Baja			NO	
						Anual									
				Nunca											
Usuario	Se tienen establecido políticas de cambio de claves de acceso a los usuarios de los sistemas de información como sistema de la entidad, correos electrónicos etc.	SI	✓	Cada qué periodo de tiempo lo realiza	30 días		Las contraseñas que mantiene para el ingreso a los sistemas de información, principalmente sistema de la entidad y correo electrónico se considera un sistema de seguridad:	Alta	✓	El sistema de la entidad permite que las claves de acceso tengan un determinado tiempo de caducidad y por lo tanto notificar al usuario que se debe realizar cambios	SI	✓			
					60 días	✓			Media						
Funcionario Becas		NO				180 días					Baja			NO	
						Anual									
				Nunca											
Usuario	Se tienen establecido políticas de cambio de claves de acceso a los usuarios de los sistemas de información como sistema de la entidad, correos electrónicos etc.	SI	✓	Cada qué periodo de tiempo lo realiza	30 días		Las contraseñas que mantiene para el ingreso a los sistemas de información, principalmente sistema de la entidad y correo electrónico se considera un sistema de seguridad:	Alta	✓	El sistema de la entidad permite que las claves de acceso tengan un determinado tiempo de caducidad y por lo tanto notificar al usuario que se debe realizar cambios	SI	✓			
					60 días	✓			Media						
Funcionario Becas		NO				180 días					Baja			NO	
						Anual									
				Nunca											
Usuario	Se tienen establecido políticas de cambio de claves de acceso a los usuarios de los sistemas de información como sistema de la entidad, correos electrónicos etc.	SI	✓	Cada qué periodo de tiempo lo realiza	30 días		Las contraseñas que mantiene para el ingreso a los sistemas de información, principalmente sistema de la entidad y correo electrónico se considera un sistema de seguridad:	Alta	✓	El sistema de la entidad permite que las claves de acceso tengan un determinado tiempo de caducidad y por lo tanto notificar al usuario que se debe realizar cambios	SI	✓			
					60 días	✓			Media						
Funcionario TICS		NO				180 días					Baja			NO	
						Anual									
				Nunca											

REALIZADO POR: AMOY	FECHA: 23-08-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

CRONOGRAMA DE ACTIVIDADES DE METAS Y OBJETIVOS DE LA UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN

La unidad de TICs dispone de un cronograma de actividades metas y objetivos a seguir para el adecuado funcionamiento de la unidad.

No.	Objetivo Operativo	Indicador	Metas												Descripción del Indicador	Proyecto	Fase Actual	
			Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic				
1	Incrementar la efectividad en resolución de incidentes en servicios de la Gerencia de TIC MEDIANTE la implementación de mejoras en la mesa de ayuda.	1.1. Efectividad en resolución de Incidentes	0	0	0	0	0	0	0	0	70	75	80	82	85	Agilizar la atención a los usuarios Mejorar el servicio de soporte en Hardware y software Diagnóstico de problemas y posibles soluciones en el menor tiempo. Incidente = afectación al normal desenvolvimiento operacional.	1001. Implementación de mejoras en la mesa de ayuda	Completado

REALIZADO POR: AMOY	FECHA: 15-09-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

2	Incrementar la sistematización de procesos institucionales MEDIANTE el desarrollo y/o adquisición de sistemas informáticos.	2.1. Porcentaje de personal de crédito y becas capacitado en sistemas informáticos institucionales												50	Medir el porcentaje de servidores capacitados, que pertenecen a las áreas agregadoras de valor, en sistemas informáticos que la institución utiliza	I005. Sistematización del Proceso de Otorgamiento y Administración de los Créditos y Becas del IECE	Ejecución
		2.2. Número de módulos desarrollados y /o que reciben mantenimiento	1	2	2	3	3	4	7	7	7	7	7	7	7	Módulo de Administración del Sistema Módulo Administrativo Financiero Módulo de Crédito Módulo de Becas Módulo de Coactivas Módulo de RRHH Módulo de Cumplimiento	Completado

REALIZADO POR: AMOY	FECHA: 15-09-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

INVENTARIO DE HARDWARE

N°	NOMBRE DE EQUIPO	USUARIO	DIRECCION IP	DOMINIO	DEPRATAMENTO
1	MLASCANO	MLASCANO	10.10.16.2	IECE	CREDITO
	ITEM	EQUIPO	MARCA	MODELO	SERIE
	1	CPU	HP	HP COMPAQ dc7900	SMXJ0010BSJ
	2	Monitor	HP	LE1901w	S3CQ9222P56
	3	Teclado	HP	USB	BAUHR0HVBYB1FV
	4	Mouse	HP	USB	FATSK0K5DY6GH0
	5	Telefono IP	CISCO	7945	FCH1549B74R
2	AGAIBOR	AGAIBOR	10.10.16.22	IECE	COACTIVAS
	ITEM	EQUIPO	MARCA	MODELO	SERIE
	1	CPU	HP	HP COMPAQ dc5800	MXJ84408MC
	2	MONITOR	HP	L1910	CNC838NW4W
	3	TECLADO	HP	PS/2	BC3370GVBWD0SR
	4	MOUSE	HP	PS/2	FB7330AN3WD26SM
	5	TELEFONO IP	CISCO	7945	FCH15518KDK
3	MMUNOZ	MMUNOZ	10.10.16.2	IECE	JURIDICO
	ITEM	EQUIPO	MARCA	MODELO	SERIE
	1	CPU	HP	HP COMPAQ dc7900	SMXJ0010BRD
	2	MONITOR	HP	LE1901W	S3CQ9222P5G
	3	TECLADO	HP	USB	BAUHR0HVBYB1AF
	4	MOUSE	HP	USB	FATSK0K5DY6GXL
	5	TELEFONO IP	CISCO	7945	FCH1551A45Z
4	MGOYES	MGOYES	10.10.16.18	IECE	TESORERIA
	ITEM	EQUIPO	MARCA	MODELO	SERIE
	1	CPU	HP	HP COMPAQ dc5800	MXJ846062X
	2	MONITOR	HP	L1910	CNC838NVJO
	3	TECLADO	HP	PS/2	BC3370GVBWH494
	4	MOUSE	HP	PS/2	FB7330AN3WHOHTF
	5	IMPRESORA	EPSON	EPSON TM-U210D	FFF6032955
6	TELÉFONO IP	CISCO	7945		

La unidad de TICs dispone de un inventario adecuado de hardware.

REALIZADO POR: AMOY	FECHA: 22-09-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

INVENTARIO DE SOFTWARE

INVENTARIO DE SOFTWARE	
Sistema de Crédito Educativo (SIGEN)	
Permite:	
➤	Concesión
➤	Desembolso
➤	Recuperación
Delta 21 Automatiza todos los programas de becas existentes.	
ZIMBRA	Correo electrónico.
ARANDA	Sistema de soporte.
QUIPUX	Gestión documental
SITAC	Sistema contable
GOIA	Soluciones tecnológicas
GPR	Gobierno por resultados
INCOP	Compras publicas

Este software permite desarrollar las actividades en la entidad, si existe alguna falla en los mismos se solucionan comunicando a la matriz.

REALIZADO POR: AMOY	FECHA: 22-09-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS (IECE) REGIONAL 3 RIOBAMBA
INSPECCIÓN FÍSICA

UNIDAD: <i>Administrativa y Financiera</i>									
CPU		MONITOR		TECLADO		MOUSE		TELÉFONO IP	
Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple
UNIDAD: <i>Administrativa y Financiera</i>									
CPU		MONITOR		TECLADO		MOUSE		TELÉFONO IP	
Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple
UNIDAD: <i>Jurídica Coactivas</i>									
CPU		MONITOR		TECLADO		MOUSE		TELÉFONO IP	
Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple
UNIDAD: <i>Jurídica Coactivas</i>									
CPU		MONITOR		TECLADO		MOUSE		TELÉFONO IP	
Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple
UNIDAD: <i>Crédito</i>									
CPU		MONITOR		TECLADO		MOUSE		TELÉFONO IP	
Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple
UNIDAD: <i>Beças</i>									
CPU		MONITOR		TECLADO		MOUSE		TELÉFONO IP	
Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple
UNIDAD: <i>Tics</i>									
CPU		MONITOR		TECLADO		MOUSE		TELÉFONO IP	
Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple	Cumple ✓	No cumple

REALIZADO POR: AMOY	FECHA: 22-09-2013
REVISADO POR: BNCO	FECHA: 18-12-2013

ANEXOS

ANEXO 1

ENCUESTAS PARA EL ANÁLISIS SITUACIONAL

ENCUESTA AL GERENTE DEL IECE

FECHA: 02/07/2017.....

CARGO: Gerente.....

OBJETIVO: Identificar las actividades realizadas por la gerencia en lo referente a la administración del área informática del IECE

1. ¿Considera usted que la situación actual del área informática contribuye al cumplimiento de la misión y visión institucional?
 Totalmente
 Parcialmente
 No contribuye
2. ¿Considera usted que el área de sistemas cuenta con personal profesional y capacitado?
 Si
 No
3. ¿Se han producido problemas o deficiencias significativas en las funcionalidades ofrecidas por los sistemas?
 Si
 No
4. ¿En caso afirmativo, se han establecido procedimientos alternativos?
 Si
 No
5. ¿Cuentan con un plan de inversión periódica referente a la adquisición y equipamiento del área Informática?
 Siempre
 Frecuentemente
 Ocasionalmente
 Nunca
6. ¿Considera usted que se cuenta con un área de informática adecuada en la entidad?
 Totalmente
 Satisfactoriamente
 Poco satisfactorio
 Insatisfactorio

12. ¿Considera usted que es importante cambiar las claves de acceso a los sistemas de

7. ¿Se dispone de Software aplicativos (programas) en el área de sistemas para la correcta ejecución de las actividades en la institución?

- Totalmente
- Satisfactoriamente
- Poco satisfactorio
- Insatisfactorio

8. ¿Considera que el área de sistemas es el adecuado para cumplir con los expectativas propuestas por el estado ecuatoriano en cuanto al desempeño de la entidad?

- Totalmente
- Parcialmente
- No cumple

9. ¿De acuerdo a la creciente demanda de los clientes de la institución considera usted que el área de sistemas satisface los requerimientos de los funcionarios y los clientes?

- Totalmente
- Satisfactoriamente
- Poco satisfactorio
- Insatisfactorio

10. ¿En la adquisición de infraestructura tecnológica que personal interviene para establecer las necesidades del área de sistemas? (Escoja varias opciones)

- Gerente
- Jefes departamentales
- Técnicos
- Otros

11. ¿Considera que la información interna de la institución está protegida contra posibles daños ocasionadas por personas ajenas a la institución?

- Si
- A veces
- No

12. Las claves de acceso a los sistemas de información son asignadas por:

- Autoridades de la institución
- Técnicos del área de sistemas
- Por cuenta propia de los funcionarios
- Otros

13. ¿Considera usted que es importante cambiar las claves de acceso a los sistemas de información por motivos de seguridad?
- Si
 No
14. ¿Si su respuesta es afirmativa. Realiza Ud. Dichos cambios?
- Si
 A veces
 No
15. ¿Considera usted que existen las medidas de seguridad adecuadas a fin de salvaguardar y evitar pérdidas de los equipos informáticos en la entidad?
- Totalmente
 Parcialmente
 Inexistente
16. ¿Considera usted que el servicio de internet dentro de la institución satisface las necesidades de los usuarios?
- Satisfactoriamente
 Poco satisfactorio
 Insatisfactorio
17. ¿Considera usted que se brinda un adecuado mantenimiento de equipos informáticos en la institución?
- Si
 A veces
 No
18. ¿Se realiza capacitación del personal del área de sistemas de forma permanente?
- Siempre
 Parcialmente
 Nunca

ENCUESTA A LOS FUNCIONARIOS DEL IECE

FECHA: 07/07/2013

CARGO: Experta en tesorería Bancaria

OBJETIVO: Conocer las perspectivas que tienen los docentes del área informática acerca de la infraestructura tecnológica y equipamiento en los laboratorios de cómputo.

1. ¿Considera usted que los equipos informáticos de la institución están debidamente adecuados y equipados para la correcta ejecución de las actividades?
 Completamente
 Satisfactoriamente
 Poco satisfactorio
 Insatisfactorio
2. ¿Considera usted que las autoridades del IECE brindan los recursos suficientes para la adquisición y equipamiento adecuado del área de sistemas?
 Totalmente
 Parcialmente
 No cumple
3. ¿Considera que el software (programas) es el adecuado para desempeñar sus funciones?
 Totalmente
 Parcialmente
 No cumple
4. ¿Considera usted que los recursos informáticos empleados en la entidad permiten cumplir con la misión y visión de la entidad?
 Totalmente
 Parcialmente
 No cumple
5. Según a su criterio el servicio de internet del área de sistemas de la entidad es:
 Excelente
 Bueno
 Regular
 Deficiente
6. ¿Considera usted que se toman las medidas de seguridad adecuadas para evitar la pérdida o sustracción de los recursos informáticos?
 Si
 No

No CUESTA A LOS FUNCIONARIOS DEL ICEE

7. ¿Al momento que se incorporan nuevos elementos tecnológicos en la entidad se le capacita para su correcta utilización?

Completamente
 Satisfactoriamente
 Poco satisfactorio
 Insatisfactorio

8. ¿Cuentan con claves de acceso para ingresar al sistema de entidad?

Si
 No

9. ¿Se realiza mantenimiento de los recursos informáticos?

Siempre
 Ocasionalmente
 Nunca

10. ¿Considera Ud. Qué la información interna de la institución está protegida contra posibles sabotajes ocasionadas por personas ajenas a la institución?

Si
 No

ANEXO 2

CUESTIONARIO PARA ANALIZAR EL CONTROL INTERNO NOMBRE DE LA ENTIDAD

Área:

Componente:

MOTIVO DEL EXAMEN:

Nº	PREGUNTAS	REPUESTAS			COMENTARIO
		SI	NO	N/A	
TOTAL					

ANEXO 3

MATRIZ DE PONDERACIÓN NOMBRE DE LA ENTIDAD

Nº	PREGUNTAS	PONDERACIÓN	CALIFICACIÓN
TOTAL			

ANEXO 4

TABLA DE RIESGO Y CONFIANZA

TABLA DE RIESGO Y CONFIANZA		
RANGO	RIESGO	CONFIANZA
15% - 50%	ALTO	BAJO
51% - 75%	MEDIO	MODERADO
76% - 95%	BAJO	ALTO

ANEXO 5

MATRIZ DETERMINACIÓN DE ÁREAS CRÍTICAS

Detalle	Nivel de riesgo	Causa	Impacto	Acciones recomendadas	Norma relacionada

ANEXO 6

PROGRAMA DE AUDITORÍA

Entidad:

Área:

Tipo de Auditoría:

Fase:

Objetivo:

Nº	DESCRIPCIÓN	REF. PT.	ELABORADO POR:	FECHA	OBSERVACIONES
PROCEDIMIENTOS					

ANEXO 7

FICHA TÉCNICA DE INDICADORES

NOMBRE DEL INDICADOR	FACTORES CRÍTICOS DE ÉXITO	FORMULA DE CALCULO	FRECUENCIA	VALORES	%	INTERPRETACIÓN

ANEXO 8

Funciones del personal de la unidad de TICs.

Hardware:

- Formateo de computadores PC y portátiles de la regional y agencias.
- Elaborar el inventario de equipo informático de la regional y sus agencias.
- Instalación y configuración de impresoras.
- Monitoreo de la central telefónica y teléfonos IP.
- Monitoreo del correcto funcionamiento de los equipos de video conferencia.
- Monitoreo del equipo del sistema de turnos digitales.
- Monitoreo del funcionamiento del UPS local.

Software

- Brindar soporte técnico a usuarios en los aplicativos informáticos.
- Brindar soporte técnico al parque informático en la regional y agencias.
- Actualizar versiones de los sistemas institucionales SIGEN, SIB, BECAS SENESCYT.
- Instalar programas y utilitarios necesarios para el funcionamiento del equipo informático.
- Instalación y configuración de la Consola de Antivirus en Regional y Agencias.
- Configurar acceso a los sistemas institucionales.
- Configurar y habilitar puntos de acceso del sistema de turnos G.O.I.A.
- Instalación y configuración de navegadores.
- Instalación y actualización de software SRI y SITAC.
- Soporte sistema Quipux.
- Registro y seguimiento de casos sistema de soporte Aranda.

Redes

- Implementación de puntos de red.
- Configuración de acceso inalámbrico.
- Monitoreo del correcto funcionamiento de los enlaces de datos externos.
- Administración de servidores.
- Administración y configuración de servidor Linux, Samba.

- Administración y configuración de servidor de Antivirus Kaspersky.

INCOP

- Registro de compras de ínfima cuantía en el portal INCOP.
- Registro de procesos de compras públicas en el portal INCOP
- Generar orden de compra en catalogo electrónico, subasta inversa, menor cuantía, etc.

Reportes

- Elaborar reportes solicitados de la información requerida.
- Inventario de equipos informáticos de la Regional y Agencias.
- Reporte de los casos atendidos semanalmente en el sistema Aranda.
- Reporte mensual de Ínfima Cuantía.

Capacitación

- Medidas de seguridad informática y esquemas de seguridad.
- Capacitación de IPv6.
- Capacitación de medidas de evaluación de desempeño de equipos de comunicaciones y servidores.
- Capacitación de Compras públicas.
- Capacitación de Contraloría General del Estado: Gestión Pública.
- Capacitación de Contraloría General del Estado: Administración por procesos, diagramación y manejo de Visio.
- Capacitación de Contraloría General del Estado: Ética Pública.
- Capacitación de Contraloría General del Estado: Auditoría en ambiente informático.
- Capacitación en PMBOOK.
- Capacitación de normas ISO 27000
- Capacitación del cableado estructurado.
- Capacitación de COBIT, etc.

ANEXO 9



MEMORANDO No. 235-GTIC-2012

PARA: Dr. Fabián Solano Moreno
GERENTE GENERAL IECE

DE: Ing. Esteban Torres
GERENTE DE TIC
PRESIDENTE DEL COMITÉ DE INFORMÁTICA

FECHA: 2012-08-13

Quote TICs.
Continuación
Trámite Digitalización
14. 08-2012
Solano
Seguimiento

De acuerdo a la sumilla inserta en el Memorando No. 358-SG-2012 de 26 de julio del año en curso, mediante la cual se me designa para presidir el Comité de Informática, cúpleme remitir para su conocimiento y aprobación, las políticas de los sistemas de información y comunicación, así como también el acta de la reunión del Comité de Informática reunido el 30 de julio del 2012, mediante la cual el Comité resolvió poner en consideración de su autoridad dichas políticas.

Atentamente,

Ing. Esteban Torres Romo
GERENTE DE TIC
PRESIDENTE DEL COMITÉ DE INFORMÁTICA

SECRETARIA GENERAL
RECIBIDO
POR: *[Signature]*
FECHA: 15 AGO 2012
HORA: 15:17

Secretario General
para conocimiento
a nivel nacional
ARRAIZA
[Signature]
14/08/12

E/c.

SECRETARIA GENERAL
RECIBIDO
15 AGO 2012
[Signature]

SECRETARIA GENERAL
14 AGO 2012
[Signature]
[Signature]

ANEXO 10



RESOLUCIÓN No. 29-GG-IECE-2012

EL GERENTE GENERAL DEL INSTITUTO ECUATORIANO DE
CREDITO EDUCATIVO Y BECAS, IECE.

CONSIDERANDO

Que, la Constitución de la República del Ecuador en el Art. 227: "La administración Pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad...";

Que, mediante Resolución 030-DIR-IECE-2012, de 22 de Junio de 2012, el Directorio del IECE aprobó el ESTATUTO ORGANICO DE GESTIÓN POR PROCESOS de la Entidad;

Que, mediante Oficio No. 5803 MRL-FI-2012-EDT, de 15 de Agosto de 2012, el Ministerio de Relaciones Laborales, emite el dictamen favorable al proyecto de reforma al Estatuto Orgánico de Gestión Organizacional del IECE;

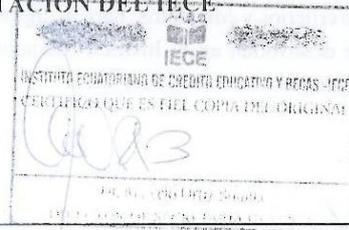
Que, el Art. 21 del Estatuto Orgánico de Gestión por Procesos señala: "De la Secretaría General.- Misión: "Certificar los actos administrativos y normativos expedidos por la institución; custodiar y salvaguardar la documentación de propiedad del IECE";

Que, es importante establecer procesos de digitalización de la documentación institucional, a fin de optimizar los recursos, reducir el traslado de papel, evitar la manipulación indebida de la documentación, minimizar el deterioro del papel y especialmente reducir los costos y el tiempo de servicio de los beneficios internos y externos de forma eficiente y eficaz; y,

Que, En uso de las atribuciones que le confiere la Ley Sustitutiva a la Ley del IECE, en el Art.10: "Son atribuciones y deberes del Gerente General:" literal m) "Ejercer las acciones administrativas o judiciales que se requieran para el buen funcionamiento de la institución"...y en concordancia con los Arts. 21 y 21.1 del Estatuto Orgánico de Gestión por Procesos.

RESUELVE

Expedir el presente: **MANUAL DEL USUARIO PARA LA DIGITALIZACIÓN DE LA DOCUMENTACIÓN DEL IECE**



ANEXO 11



INSTITUTO ECUATORIANO DE
CRÉDITO EDUCATIVO Y BECAS

RESOLUCIÓN 024-DIR-IECE-2008

EL DIRECTORIO DEL INSTITUTO ECUATORIANO DE CRÉDITO EDUCATIVO Y BECAS - IECE

CONSIDERANDO:

- Que, con Resolución CNA-001-2005 de 13 de junio de 2005, publicada en el R.O. 67 de 25 de julio de 2005, el Consejo Nacional de Archivos expide el Instructivo de Organización Básica y Gestión de Archivos Administrativos, de conformidad con lo dispuesto en la Ley Orgánica y Reglamento General de Transparencia y Acceso a la Información Pública;
- Que, dicho Instructivo es de uso y aplicación obligatoria en todos los organismos, entidades e instituciones del sector público y privado con participación del Estado;
- Que, el Instructivo en referencia, no establece los plazos de conservación documental, por lo que en el marco de las actividades que realiza la Entidad, es necesario contar con disposiciones que normen el proceso de clasificación y conservación de documentos de uso permanente y temporal, así como de eliminación de aquellos que han perdido su valor por haber dejado de tener incidencia legal, técnica, financiera, administrativa, estadística o de otra índole;
- Que, en el Archivo Pasivo del IECE existen documentos que deben ser eliminados, por cuanto ya han cumplido con el propósito para el cual fueron emitidos; son de carácter transitorio y ya no son motivo de consulta alguna, ni mucho menos pasar a constituirse en un Archivo Histórico Institucional; y,
- En ejercicio de las atribuciones que le confiere el literal d) del Art. 7 de la Ley Sustitutiva a la Ley del IECE,

RESUELVE:

Expedir el siguiente **Reglamento para la Selección y Eliminación de Documentos de Propiedad del IECE.**

Art. 1.- AMBITO.- El presente Reglamento tiene un ámbito de aplicación nacional y cuyo propósito es normar el proceso de selección, evaluación, conservación y eliminación de documentos que han perdido su valor permanente.

Art. 2.- ENVÍO DE DOCUMENTOS.- Todas las unidades remitirán al Archivo Pasivo del IECE, en caja de cartón, los documentos que hayan cumplido un tiempo de permanencia de tres (3) años en la unidad, contados a partir de la fecha de emisión; mediante acta entrega-recepción, por duplicado, en la que se describirá un resumen del contenido de los mismos.