ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

ESCUELA DE CONTABILIDAD Y AUDITORÍA

INGENIERÍA EN CONTABILIDAD Y AUDITORÍA C.P.A.

TRABAJO DE TITULACIÓN

Previo a la Obtención del Título de:

INGENIERO EN CONTABILIDAD Y AUDITORÍA C.P.A.

TEMA:

"AUDITORÍA DE SISTEMAS INFORMÁTICOS EN LA COOPERATIVA DE AHORRO Y CRÉDITO "EDUCADORES DE CHIMBORAZO" LTDA., DE LA CIUDAD DE RIOBAMBA, PROVINCIA DE CHIMBORAZO PARA EL PERÍODO 2014".

AUTOR:

MICHAEL ADRIÁN ERAZO GRANIZO

RIOBAMBA - ECUADOR

2015

CERTIFICACIÓN DEL TRIBUNAL

Certificamos que el presente trabajo de investigación, previo a la obtención del título de Ingeniero en Contabilidad y Auditoría C.P.A. ha sido desarrollado por el **Sr. Michael Adrián Erazo Granizo**, ha cumplido con las normas de investigación científica y una vez analizado su contenido, se autoriza su presentación.

Ing. Hítalo Bolívar Veloz Segovia

DIRECTOR

Ing. Mercedes Leticia Lara Freire

MIEMBRO

DECLARACIÓN DE AUTENTICIDAD

Yo, Michael Adrián Erazo Granizo, declaro que el presente trabajo de titulación es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente, están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este trabajo de titulación.

Riobamba, 01 de diciembre del 2015

Michael Adrián Erazo Granizo
060411997-4

DEDICATORIA

A mis amados padres Teresa y Arturo, por ser las personas más importantes para mí, siempre estuvieron y estoy seguro que estarán apoyándome en cada proyecto de mi vida.

A mis abuelos por acogerme y guiarme con sus conocimientos, experiencias y consejos.

A toda mi familia, en especial a mi tía Marisol; además a todas aquellas buenas personas que conozco, porque de cada uno aprendí algo que me ayudó a ser mejor.

A mis amigos y amigas, a ustedes gracias compartir conmigo las alegrías y las penas que da la vida y seguir con una sonrisa sincera a mi lado.

A toda aquellas maravillosas personas quienes han sido mis maestros y maestras durante toda mi vida, por guiarme y adiestrarme desde niño hasta ahora la adultez; tantos nombres que se hacen imposibles de citar pero que nunca serán olvidados.

Michael A. Erazo G.

AGRADECIMIENTO

A la vida, por permitirme estar aquí para compartir con las personas que quiero y poder cumplir mis objetivos.

A mis amados padres, por ser el apoyo más grande proporcionándome todo aquello que necesité desde niño hasta hoy que estoy culminando mi carrera.

A mis amigos de toda la vida y aquellos que conocí en mi vida universitaria por estar siempre ahí apoyándonos y creyendo el uno en el otro.

A todos mis profesores, por educarme desde siempre.

A quiénes laboran en la Cooperativa de Ahorro y Crédito “Educadores de Chimborazo Ltda.”, por su ayuda desinteresada y su buena voluntad demostrada en la realización del presente trabajo.

ÍNDICE DE CONTENIDO

ÍNDICE DE CUADROS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN EJECUTIVO

En el presente trabajo de investigación se realizó una auditoría de sistemas informáticos en la cooperativa de ahorro y crédito educadores de Chimborazo Ltda., de la ciudad de Riobamba, provincia de Chimborazo, para determinar el grado de confianza de la información recopilada, procesada y entregada, determinar respecto a la economía, eficiencia y eficacia de la utilización de los recursos tecnológicos, y comprobar si se cumple o no con las normas más elementales de control.

Se recopiló la información necesaria mediante la aplicación de herramientas investigativas como la entrevista, observación y cuestionarios; a través de éstas se pudo determinar los hallazgos que cuentan con evidencia suficiente y competente como sustento al trabajo desempeñado.

La baja aplicación de los planes de capacitación continua para el manejo d las tecnologías de la información y comunicación, manuales de funciones no alineados a los intereses de las tecnologías, inexistencia de un marco de trabajo de administración de riesgos, no seguimiento por parte de auditoría interna al departamento de sistemas, infracciones en las obligaciones de los técnicos, falta de presupuesto y de apoyo en ciertos aspectos relevantes, ingresos no registrados a la información de sistemas, control de errores conforme los mismos se presentan, son los más relevantes para la entidad.

Se recomienda que la entidad contrate una auditoría informática por parte de una firma auditora certificada y acreditada para la evaluación de sus sistemas y así conozca el estado de los mismos, tome correctivos y a su vez consiga una certificación que acredite la valía de las transacciones que ejecuta.

Palabras claves: auditoría informática, sistema informático, marco de trabajo de administración de riesgos.

Ing. Hítalo Bolívar Veloz Segovia
DIRECTOR TRABAJO TITULACIÓN

SUMMARY

This research work is an audit of the computer system at Savings and Credit Cooperative "Educadores de Chimborazo" Ltda. in the city of Riobamba, Chimborazo Province. The objective is to determine the reliability level of the compiled, processed and submitted information concerning the economy, efficiency and efficacy of technological resources. The goal is also to prove whether the cooperative complies or not with the elemental control regulations.

The necessary information was compiled through different research tools such as interviews, observation and questionnaires; with these elements it was plausible to determine the evidences to support this work.

Some of the most relevant observations detected were as follows: there is low application of permanent training plans for the use of communication and information technologies; the duty handbooks do not match technology interests; there is absence of a framework of risk management; the systems department is not being monitored by the internal audit office; the technicians infringe their responsibilities, there is lack of economic resources and support to some relevant aspects; there is some income that has not been registered in the system; and, there is no error observing as they occur.

It is recommended that the Cooperative hires systems auditors that work for a well-known and certified audit company to make a good evaluation of their systems in order to consider the possibility to get a certification that guarantees the well management of the Cooperative transactions.

Key words: systems audit, information system, framework of risk management.

INTRODUCCIÓN

En los tiempos modernos no se puede negar que la tecnología se ha convertido en un aliado poderoso y casi imprescindible al momento de cumplir con las actividades económicas que dan el sustento al ser humano.

Más que ningún otro, el sector financiero ha sido el que más influencia y beneficios ha recibido de la implantación de las nuevas tecnologías, ya que permiten gestionar de manera rápida, eficiente y barata toda la información y el conjunto de transacciones que a diario se realizan en los bancos, financieras, mutualistas, cooperativas y otros similares.

Es por ello que se ha escogido a la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda. de la ciudad de Riobamba, provincia de Chimborazo, con el fin de realizar una auditoría y así determinar el grado de economía, eficiencia y eficacia de la utilización de los recursos tecnológicos pertenecientes a la misma.

En el primer capítulo detalla cual es la situación actual de la cooperativa y cuál va a ser el fin de ésta evaluación, así como los objetivos que se persiguen con la misma.

En el segundo capítulo se detalla la información formal y de carácter científico que servirá de base para la investigación, éstas son las Normas COBIT 4.1 y las Normas ISO 27002, que si bien no son una normativa legalmente aprobada si sirven como marco de referencia para determinar los puntos que deberán ser evaluados y luego recomendar las soluciones necesarias.

El capítulo tres abarca la metodología que se utilizará con el fin de culminar la investigación, y así estandarizar el trabajo y se mantenga un formato compacto.

Finalmente se emitirá un informe que será entregado oportunamente a la parte interesada para que mejore sus procesos actuales, garantizando su mejora y permanencia en el mercado financiero.

CAPÍTULO I: EL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

1.1.1 Formulación del problema

¿La elaboración de una auditoría de sistemas informáticos en la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda., de la ciudad de Riobamba, provincia de Chimborazo para el período 2014 permitirá dictaminar respecto a la economía, eficiencia y eficacia de la utilización de los recursos tecnológicos?

1.1.2 Delimitación del problema

El presente trabajo se lo realizará en la ciudad de Riobamba, provincia de Chimborazo.

Campo: Auditoría

Área: Auditoría informática

Temporal: Período 2014

Espacial: Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda.

1.2 JUSTIFICACIÓN

La auditoría consiste principalmente en el estudio de los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos. Los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia. Particularmente la parte Informática hoy, está subsumida en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar, por lo tanto, sometidos a los generales de la misma. Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma, entonces, debido a su importancia en

el funcionamiento de una empresa, existe la Auditoría Informática. Los principales objetivos que constituyen a la auditoría Informática son el control de la función informática, el análisis de la eficiencia de los Sistemas Informáticos que comporta, la verificación del cumplimiento de la Normativa general de la empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos informáticos.

En el desarrollo normal de las operaciones de una institución del sector financiero se requiere una constante vigilancia y evaluación; asimismo, se necesita de una opinión, preferiblemente independiente, que les ayude a medir la eficiencia y eficacia en el cumplimiento de sus objetivos. La auditoría de sistemas informáticos contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones; la revisión analítica a la suficiencia de controles establecidos en el ámbito informático, con la finalidad de disminuir los riesgos y garantizar la seguridad, confiabilidad y exactitud de la información.

Queda claro entonces que una revisión de este tipo sería propicia para que la alta gerencia compruebe a través del respectivo informe si sus procesos y decisiones actuales han entregado los resultados más idóneos, o si por el contrario han producido alteraciones sobre las cuales se deben tomar correctivos inmediatos, y así poder garantizar que los sistemas informáticos de la entidad generen información que sea certera, útil, y segura tanto para los clientes internos y externos de la entidad.

La Cooperativa de Ahorro y Crédito “Educadores de Chimborazo” Ltda. perteneciente a la categoría 2 dentro de las cooperativas de ahorro y crédito del sistema financiero nacional ha planteado la necesidad de la aplicación de este tipo de auditoría a través de su gerente, ya que previamente nunca se ha ejecutado este tipo de examen dentro de sus instalaciones y no conocen su estado actual en este ámbito, además la información que reciban será usada para detectar sus falencias y combatirlas, incrementar la calidad y cantidad de sus puntos fuertes, aprovechar las oportunidades que se generen en el entorno y estar mejor preparados para eventuales amenazas que pudiesen suscitarse a futuro, dejando atrás prácticas improvisadas o empíricas y dando paso a la generación de información, que se constituya uno de los activos más valiosos para la institución.

1.3 OBJETIVOS

1.3.1 Objetivo general

- Elaborar una auditoría de sistemas informáticos en la Cooperativa de Ahorro y Crédito “Educadores de Chimborazo” Ltda., de la ciudad de Riobamba, provincia de Chimborazo para el período 2014 para dictaminar respecto a la economía, eficiencia y eficacia de la utilización de los recursos tecnológicos.

1.3.2 Objetivos específicos

- Estructurar un marco teórico referencial que contribuya al desarrollo de la presente investigación.

- Aplicar la norma COBIT 4.1 y la norma ISO 27002, a fin de detectar la existencia de vulnerabilidades en los recursos de tecnologías de la información.

- Emitir un informe mostrando las respectivas conclusiones y recomendaciones que permita a la gerencia y al personal tomar los correctivos pertinentes.

CAPÍTULO II: MARCO TEÓRICO

2.1 ANTECEDENTES INVESTIGATIVOS

2.1.1 Antecedentes históricos

Historia

En el mes de marzo de 1964, en la Oficina de la Inspección Escolar nace la idea de formar una Cooperativa de Ahorro y Crédito para los Educadores de parte del Sr. Alfonso Hernández Inspector de la Primera Zona de la ciudad de Riobamba; idea que contagió a un grupo de 30 educadores, quienes se convocan y formar la Pre - Cooperativa, siendo elegido como Presidente de la Directiva Provisional el Señor Profesor Humberto Olivo.

Transcurrido tres meses, y luego de los respectivos trámites, el Ministerio de Previsión Social y Trabajo le otorga la personería jurídica a través de Acuerdo Ministerial No. 2055 de fecha 26 de Junio de 1964 y Número de Orden 1143 de la misma fecha.

Es nombrado como primer Presidente de la Cooperativa el Sr. Gilberto Moreano y como primer Gerente el Sr. Luis Calahorrano. Las primeras resoluciones que este cuerpo colegiado toma son:

1. Que los aportes de ahorro sean descontados mensualmente a través del rol de pagos.

2. Que se invite a todos los maestros de la provincia a asociarse a la Cooperativa, y se encarga a cada uno de los miembros fundadores la difusión y captación de socios.

Las primeras reuniones se dieron en la Escuela Magdalena Dávalos de la ciudad de Riobamba. Luego pasa a funcionar la Cooperativa en un local junto a la Dirección Provincial de Educación en las calles Tarqui entre Guayaquil y 10 de Agosto.

En el año 1974, pasa a funcionar en la planta baja del Edificio Vega de las calles Colón y Guayaquil, donde funcionaba también la Dirección Provincial de Educación. Debido a que el espacio físico no prestaba las comodidades para atender eficientemente a los

socios, en el año 1980 pasa a funcionar en la planta baja del Edificio llamado el Reloj de Lara en las calles España y Veloz esquina.

La Cooperativa desde sus inicios forma parte de la Federación Ecuatoriana de Cooperativas de Ahorro y Crédito – FECOAC y del Banco de Cooperativas, del cual obtiene un préstamo de dos millones de sucres para conceder créditos a sus socios.

En el año de 1967 se crea el Comisario de la Cooperativa, con la participación de dos empleados, el mismo que fue creciendo y que tuvo que liquidarse en el año de 2002, por malos manejos administrativos.

El 8 de Octubre de 1981, se adquiere el edificio de las calles Veloz y Espejo esquina a la Familia Cedeño Corral por un valor de S/. 1.450.000,00 (un millón cuatrocientos cincuenta mil sucres), en la Presidencia del Sr. Lic. Don Eudoro Fuemayor Ruiz y la Gerencia del Profesor Cristóbal Ángel Díaz, luego de las adecuaciones necesarias la Cooperativa pasa a funcionar en su local propio.

El 24 de Septiembre de 1993, en la Presidencia de la Lic. Flérida Silva Chávez y la Gerencia del Lic. Hernán León Vizuete se adquiere el terreno aledaño a la Cooperativa a las herederas del Sr. Rafael Rodríguez Castillo por un valor de 30 millones de sucres.

En el período 2001 – 2002, Presidida por la Lic. Flerida Silva Chávez y la Gerencia del Lic. Hernán León Vizuete se construye el Edificio nuevo con la idea de proporcionar a los socios un servicio eficiente y de calidad.

En el 2003 en la administración del Lic. Carlos Delgado en calidad de Presidente e Ing. Guillermo Osorio Gerente, se realiza la remodelación de la planta baja del edifico nuevo, y pasa a funcionar las oficinas operativas de la institución.

En el mes de mayo del año 2007, la Cooperativa fue intervenida por la Dirección Nacional de Cooperativas por la ingobernabilidad existente entre sus directivos. El CPA. Galo Vinueza fue nombrado Interventor por un período de 6 meses (mayo a octubre de 2007). En el mes de noviembre del mismo año una vez terminada la intervención convoca a elecciones para elegir a los Representantes a la Asamblea General.

En el mes de diciembre del 2007 son elegidos 27 Representantes, los mismos que pasan a conformar el Consejo de Administración y Vigilancia y las Comisiones Especiales de: Crédito, Educación, Asuntos Sociales y Deportes y Jurídico Legal. Recayendo la Presidencia del Consejo de Administración en la persona del Abg. Juan Vicente Moscoso Montero y del Consejo de Vigilancia al Ing. Pedro Fabián Cazorla Machado.

En el año 2008, se nombra como Gerente General de la Cooperativa al Ingeniero Magister César Alfonso Oña Mendoza. Se incrementa el monto del Crédito Ordinario de $ 5.000,00 a $ 8.000,00, el Fondo Mortuorio de $ 500 a $ 1.500 y la ayuda mortuoria de $ 100 a $ 300. Se implementa el seguro de desgravamen para todos los créditos que la Cooperativa otorga, con una cobertura total. Se entrega el bono navideño y los intereses a los socios en efectivo, a través de la libreta libre ahorro – libre retiro por un monto de $ 336.000,00. La Cooperativa es Sede de los III Jornadas Deportivas de la Unión de Cooperativas de Ahorro y Crédito del Magisterio Ecuatoriano – UCACME.

Durante el año 2009, la Cooperativa tiene representación ante la FECOAC con un Vocal Principal en el Consejo de Vigilancia, se aprueba en Asamblea de Representantes la Gran Rifa Cooperativista en donde se rifa un vehículo chevrolet Spark II modelo 2010 y un paquete de electrodomésticos; la misma que se llevó a cabo el 30 de enero del año 2010 siendo la ganadora la Máster Piedad Orozco.

Se firma el Convenio con al Banco Central del Ecuador para integrar el Sistema de Pagos Interbancarios – SPI, el mismo que nos permite pagar los sueldos de los empleados del sector público, principalmente del sector del magisterio de la provincia de Chimborazo, así como también transferencias interbancarias y el manejo de las remesas del exterior. Se realiza una Alianza estratégica con el Banco del Austro para la implementación de un cajero automático, mismo que se cristaliza el día 25 de junio de 2010. En Febrero del mismo año, la Asamblea de Representantes institucionaliza la Gran Rifa Cooperativa.

En Marzo del 2010, son elegidos 43 Asambleístas, de los cuales se conformó el Consejo de Administración, recayendo la Presidencia en la persona del Lic. Miguel Llerena Serrano y la Presidencia del Consejo de Vigilancia en la persona del Lic. Alfonso Brito Sarmiento; entre sus principales gestiones podemos mencionar: Convenio con PROINCO para el financiamiento del CREDIROL, contactos con la Corporación

Financiera Nacional – CFN y con la Corporación Latinoamericana de Cooperativas de Ahorro y Crédito – COLAC para conseguir apalancamiento financiero, se incrementó los montos de crédito Ordinario de 8.000 a 14.000 dólares, entrega de un Vehículo Chevrolet Aveo Family al Profesor Ángel Guzmán Vélez, socio inversionista ganador de la Gran Rifa Cooperativa, efectuada el 29 de Enero del 2011.

Misión

"Somos una Institución Financiera que promueve la iniciativa de ahorro e inversión en el magisterio para mejorar la condición de vida de los socios".

Visión

En el año 2013, la Cooperativa liderará un Grupo Corporativo y estratégico para enfrentar los desafíos del futuro como una de las primeras Cooperativas del magisterio ecuatoriano.

Principios

- Respetar a la persona humana.

- Prioridad del servicio a los clientes.

- Mejoramiento continuo.

Valores institucionales personales

- Entusiasmo.

- Ética.

- Solidaridad.

- Liderazgo.

- Trabajo en equipo.

- Responsabilidad Social.

- Compromiso.

- Confianza.

- Integridad con eficiencia.

Valores institucionales empresariales

- Productividad.

- Creatividad e Innovación.

- Competitividad.

- Compromiso y cultura de trabajo en equipo.

- Profesionalismo.

- Integración.

- Sanidad, prudencia y transparencia financiera.

2.2 FUNDAMENTACIÓN TEÓRICA

2.2.1 Auditoría y auditoría informática

a) Auditoría

Auditoría es un proceso formal y necesario para las empresas que tiene como fin asegurar que sus activos sean protegidos en forma adecuada. Asimismo, la alta dirección espera que de los proyectos de auditoría surjan las recomendaciones necesarias para que se lleven a cabo de manera oportuna y satisfactoria las política, controles y procedimientos definidos formalmente, con objeto de que cada individuo o función de la organización opere de modo productivo en sus actividades diarias, respetando las normas generales de honestidad y trabajo aceptadas (Hernández, 2000, p. 13).

b) Auditoría informática

Es la revisión técnica, 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 realiza 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.

Cabe señalar que la auditoría informática como tal, se la puede aplicar utilizando varios métodos o sub-áreas de los cuales los siguientes serán usados para la presente investigación y se detallan a continuación: (Muñoz Razo, 2002, p. 19).

- **Auditoría con la computadora**

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 la computadora 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. (Muñoz Razo, 2002, p. 24).

- **Auditoría sin la computadora**

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. Asimismo, 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 (Muñoz Razo, 2002, p. 24).

- **Auditoría a la gestión informática**

Es la auditoría cuya aplicación se enfoca exclusivamente a la revisión de las funciones y actividades de tipo administrativo que se realizan dentro de un centro de cómputo, tales como la planeación, organización, dirección y control de dicho centro. Esta auditoría se realiza también con el fin de verificar el cumplimiento de las funciones y actividades asignadas a los funcionarios, empleados y usuarios de las áreas de sistematización, así como para revisar y evaluar las operaciones del sistema, el uso y protección de los sistemas de procesamiento, los programas y la información. Se aplica también para verificar el correcto desarrollo, instalación, mantenimiento y explotación de los sistemas de cómputo, así como sus equipos e instalaciones. Todo esto se lleva a cabo con el propósito de dictaminar sobre la adecuada gestión administrativa de los sistemas computacionales de una empresa y del propio centro informático (Muñoz Razo, 2002, p. 25).

- **Auditoría del sistema de cómputo**

Es la auditoría técnica y especializada que se enfoca únicamente a la evaluación del funcionamiento y uso correctos del equipo de cómputo, su hardware, software y periféricos asociados. Esta auditoría también se realiza a la composición y arquitectura de las partes físicas y demás componentes del hardware, incluyendo equipos asociados, instalaciones y comunicaciones internas o ex-ternas, así como al diseño, desarrollo y uso del software de operación, de apoyo y de aplicación, ya sean sistemas operativos,

lenguajes de procesamiento y programas de desarrollo, o paquetería de aplicación institucional que se utiliza en la empresa donde se encuentra el equipo de cómputo que será evaluado. Se incluye también la operación del sistema (Muñoz Razo, 2002, pp. 25-26).

- **Auditoría ISO-9000 a los sistemas computacionales**

Es la revisión exhaustiva, sistemática y especializada que realizan únicamente los auditores especializados y certificados en las normas y procedimientos ISO-9000, aplicando exclusivamente los lineamientos, procedimientos e instrumentos establecidos por esta asociación. El propósito fundamental de esta revisión es evaluar, dictaminar y certificar que la calidad de los sistemas computacionales de una empresa se apegue a los requerimientos del ISO-9000 (Muñoz Razo, 2002, p. 28).

- **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 (Muñoz Razo, 2002, p. 28).

2.2.2 Control interno y control interno informático

a) Control interno

El control interno es el establecimiento de los mecanismos y estándares de control que se adoptan en las empresas, a fin de ayudarse en la administración correcta de sus recursos, en la satisfacción de sus necesidades de seguridad, en la salvaguarda y protección de los activos institucionales, en la ejecución adecuada de sus funciones, actividades y operaciones, y en el registro correcto de sus operaciones contables y reportes de resultados financieros; todo ello para el mejor cumplimiento del objetivo institucional.

Como complemento, ahora podemos señalar esta definición de control interno con los siguientes beneficios que se obtienen con su establecimiento:

- Salvaguardar los activos de la empresa.
- Determinar los métodos y procedimientos necesarios para el buen desarrollo de sus funciones y actividades.
- Establecer la elaboración correcta de los registros contables y de los resultados financieros.
- Contribuir con la dirección de la empresa en la implantación y cumplimiento de las normas, políticas y lineamientos que regularán su actuación (Muñoz Razo, 2002, p. 106).

- **Características del control**

Para que el control en las empresas sea verdaderamente efectivo, es obligatorio considerar algunas de sus características fundamentales al momento de establecerlo.

Entre algunas de esas características encontramos:

Oportuno: Esta característica es la esencia del control, debido a que es la presentación a tiempo de los resultados obtenidos con su aplicación; es importante evaluar dichos resultados en el momento que se requieran, no antes porque se desconocerían sus verdaderos alcances, ni después puesto que ya no servirían para nada.

Cuantificable: Para que verdaderamente se puedan comparar los resultados alcanzados contra los esperados, es necesario que sean medibles en unidades representativas de algún valor numérico para así poder cuantificar, porcentual o numéricamente lo que se haya alcanzado.

Calificable: Así como los valores de comparación deben ser numéricos para su cuantificación, en auditoría en sistemas computacionales, se dan casos de evaluaciones que no necesariamente deben ser de tipo numérico, ya que, en algunos casos específicos, en su lugar se pueden sustituir estas unidades de valor por conceptos de calidad o por medidas de cualidad; mismas que son de carácter subjetivo, pero pueden ser aplicados para evaluar el cumplimiento, pero relativos a la calidad; siempre y

cuando en la evaluación sean utilizados de manera uniforme tanto para planear como para medir los resultados.

Confiable: Para que el control sea útil, debe señalar resultados correctos sin desviaciones ni alteraciones y sin errores de ningún tipo, a fin de que se pueda confiar en que dichos resultados siempre son valorados con los mismos parámetros.

Estándares y normas de evaluación: Al medir los resultados alcanzados, éstos deberán compararse de acuerdo con los estándares y normas previamente establecidos, a fin de contemplar las mismas unidades para planear y controlar; con esto se logra una estandarización que permite valorar adecuadamente los alcances obtenidos (Muñoz Razo, 2002, p. 101).

- **Objetivos del control interno**

Tomando en cuenta que el control interno busca contribuir en la seguridad y protección de los bienes de la empresa, en la obtención de información correcta y oportuna, en la promoción de la eficacia de la operación y en la dirección adecuada de la empresa, se puede establecer que su principal prioridad es la ayuda que proporciona al buen funcionamiento de la institución y a la salvaguarda de su patrimonio. Sin embargo, hace falta una información adecuada para comprobar si se satisfacen esas prioridades.

Además, el control interno también sirve para evaluar el desarrollo correcto de las actividades de las empresas, así como la aceptación y cumplimiento adecuados de las normas y políticas que regulan sus actividades.

Con base en lo anterior, se pueden establecer los siguientes puntos como los objetivos fundamentales del control interno:

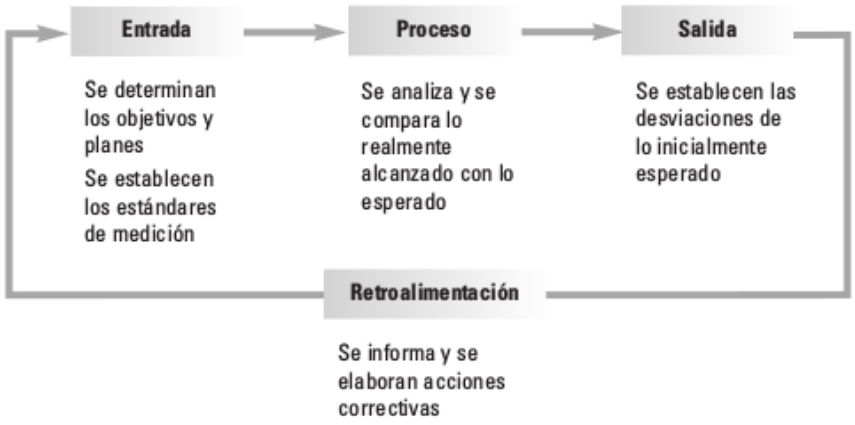
- Establecer la seguridad y protección de los activos de la empresa.
- Promover la confiabilidad, oportunidad y veracidad de los registros contables, así como de la emisión de la información financiera de la empresa.
- Incrementar la eficiencia y eficacia en el desarrollo de las operaciones y actividades de la empresa.
- Establecer y hacer cumplir las normas, políticas y procedimientos que regulan las actividades de la empresa.

- Implantar los métodos, técnicas y procedimientos que permitan desarrollar adecuadamente las actividades, tareas y funciones de la empresa (Muñoz Razo, 2002, p. 107).

- **Sistema de control**

De acuerdo con la teoría general de sistemas, entenderemos como sistema lo siguiente: "Conjunto de elementos interrelacionados que pretenden satisfacer un fin", el cual está compuesto por un ciclo fundamental de comportamiento que consiste en insumos de entrada, proceso y resultados en salidas, pero complementado con una retroalimentación que le hace corregir las posibles desviaciones encontradas (Muñoz Razo, 2002, p. 104).

Gráfico 1: El control como sistema



Fuente: Auditoría de sistemas computacionales, Carlos Muñoz Razo

b) Control interno informático

Corresponde al control específico sobre los bienes q forman parte del sistema de gestión informático.

- **Objetivos específicos**

Para hacer este análisis, propondremos los siguientes puntos como objetivos específicos del control interno informático.

- Establecer como prioridad la seguridad y protección de la información, del sistema computacional y de los recursos informáticos de la empresa.

- Promover la confiabilidad, oportunidad y veracidad de la captación de datos, su procesamiento en el sistema y la emisión de informes en la empresa.

- Implementar los métodos, técnicas y procedimientos necesarios para coadyuvar al eficiente desarrollo de las funciones, actividades y tareas de los servicios computacionales, para satisfacer los requerimientos de sistemas en la empresa.

- Instaurar y hacer cumplir las normas, políticas y procedimientos que regulen las actividades de sistematización de la empresa.

- Establecer las acciones necesarias para el adecuado diseño e implementación de sistemas computarizados, a fin de que permitan proporcionar eficientemente los servicios de procesamiento de información en la empresa (Muñoz Razo, 2002, p. 135).

- **Elementos fundamentales del control interno informático**

- Controles internos sobre la organización del área de informática.

- Controles internos sobre el análisis, desarrollo e implementación de sistemas.

- Controles internos sobre la operación del sistema.

- Controles internos sobre los procedimientos de entrada de datos, el procesamiento de información y la emisión de resultados.

- Controles internos sobre la seguridad del área de sistemas. (Muñoz Razo, 2002, p. 135).

- **Control interno en el área de informática**

Cuadro 1: Cuadro de control interno en el área de informática

Controles internos sobre la organización del área de informática • Dirección • División del trabajo • Asignación de responsabilidad y autoridad • Establecimiento de estándares y métodos • Perfiles de puestos
Controles internos sobre el análisis, desarrollo e implementación de sistemas • Estandarización de metodologías para el desarrollo de proyectos • Asegurar que el beneficio de los sistemas sea el óptimo • Elaborar estudios de factibilidad del sistema • Garantizar la eficiencia y eficacia en el análisis y diseño de sistemas • Vigilar la efectividad y eficiencia en la implementación y mantenimiento del sistema • Optimizar el uso del sistema por medio de su documentación
Controles internos sobre la operación del sistema • Prevenir y corregir los errores de operación • Prevenir y evitar la manipulación fraudulenta de la información • Implementar y mantener la seguridad en la operación • Mantener la confiabilidad, oportunidad, veracidad y suficiencia en • el procesamiento de la información de la institución

Controles internos sobre los procedimientos de entrada de datos, el procesamiento de información y la emisión de resultados

- Verificar la existencia y funcionamiento de los procedimientos de captura de datos
- Comprobar que todos los datos sean debidamente procesados
- Verificar la confiabilidad, veracidad y exactitud del procesamiento de datos
- Comprobar la oportunidad, confiabilidad y veracidad en la emisión de los resultados del procesamiento de información

Controles internos sobre la seguridad del área de sistemas

- Controles para prevenir y evitar las amenazas, riesgos y contingencias que inciden en las áreas de sistematización
- Controles sobre la seguridad física del área de sistemas
- Controles sobre la seguridad lógica de los sistemas
- Controles sobre la seguridad de las bases de datos
- Controles sobre la operación de los sistemas computacionales
- Controles sobre la seguridad del personal de informática
- Controles sobre la seguridad de la telecomunicación de datos
- Controles sobre la seguridad de redes y sistemas multiusuarios

Fuente: Auditoría de sistemas computacionales, Carlos Muñoz Razo

2.2.3 Organizaciones y normas reguladoras

Una auditoría se realiza con base a un patrón o conjunto de directrices o buenas prácticas sugeridas. Existen estándares orientados a servir como base para auditorías de informática. Uno de ellos es COBIT (Objetivos de Control de las Tecnologías de la Información), y adicional a éste podemos encontrar el estándar ISO 27002, el cual se conforma como un código internacional de buenas prácticas de seguridad de la

información, éste puede constituirse como una directriz de auditoría apoyándose de otros estándares de seguridad de la información que definen los requisitos de auditoría y sistemas de gestión de seguridad, como lo es el estándar ISO 27002 (Costas Santos, 2011, p. 27).

Además existen otras normas y estándares complementarios a las principales mencionadas anteriormente a considerarse para la presente investigación. Las mismas son detalladas a continuación:

a) COBIT

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

COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de la misma (COBIT, 2007, p. 8).

- **Misión**

Investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento (COBIT, 2007, p. 9).

- **Orientación de COBIT**

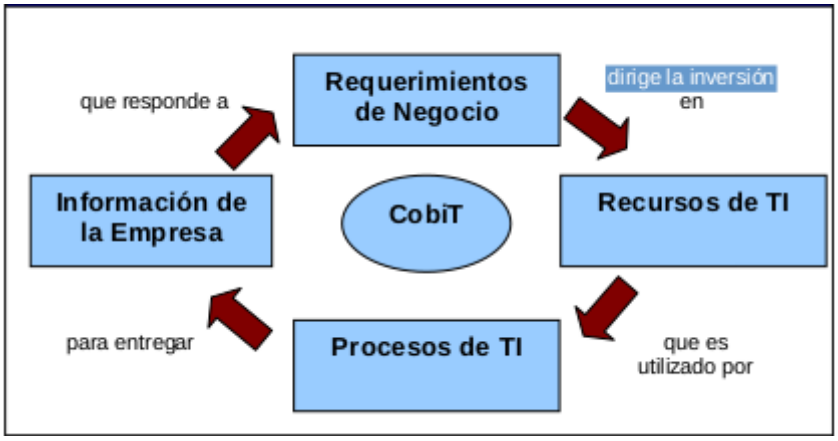
COBIT se creó con las características principales de ser orientado a negocios, orientado a procesos, basado en controles e impulsado por mediciones.

Orientación al negocio: La orientación a negocios es el tema principal de COBIT. Está diseñado para ser utilizado no sólo por proveedores de servicios, usuarios y auditores de

TI, sino también y principalmente, como guía integral para la gerencia y para los dueños de los procesos de negocio.

El marco de trabajo COBIT se basa en el siguiente principio: Para proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita invertir en, y administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que provean los servicios que entregan la información empresarial requerida (COBIT, 2007, pp. 10-11).

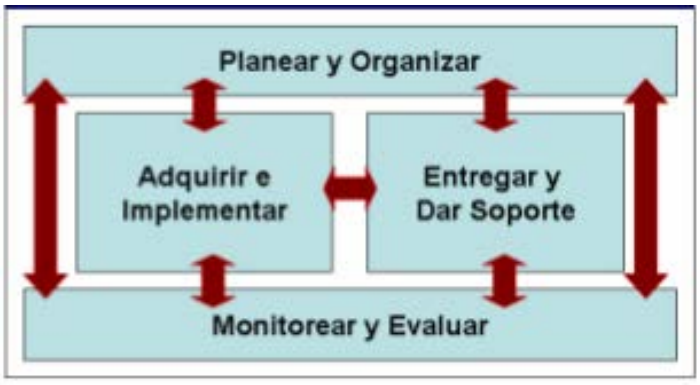
Gráfico 2: Principio básico de COBIT



Fuente: IT Governance Institute. COBIT v.4.1

Orientación a procesos: Orientado a Procesos COBIT define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios. Estos dominios son Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear (COBIT, 2007, p.12).

Gráfico 3: Los cuatro dominios interrelacionados del COBIT

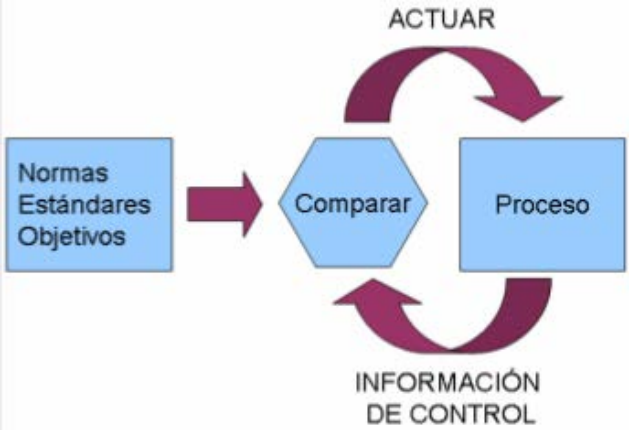


Fuente: IT Governance Institute. COBIT v.4.1

Basado en controles: Control se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos.

Los objetivos de control de TI proporcionan un conjunto completo de requerimientos de alto nivel a considerar por la gerencia para un control efectivo de cada proceso de TI (COBIT, 2007, p. 13).

Gráfico 4: Modelo de control

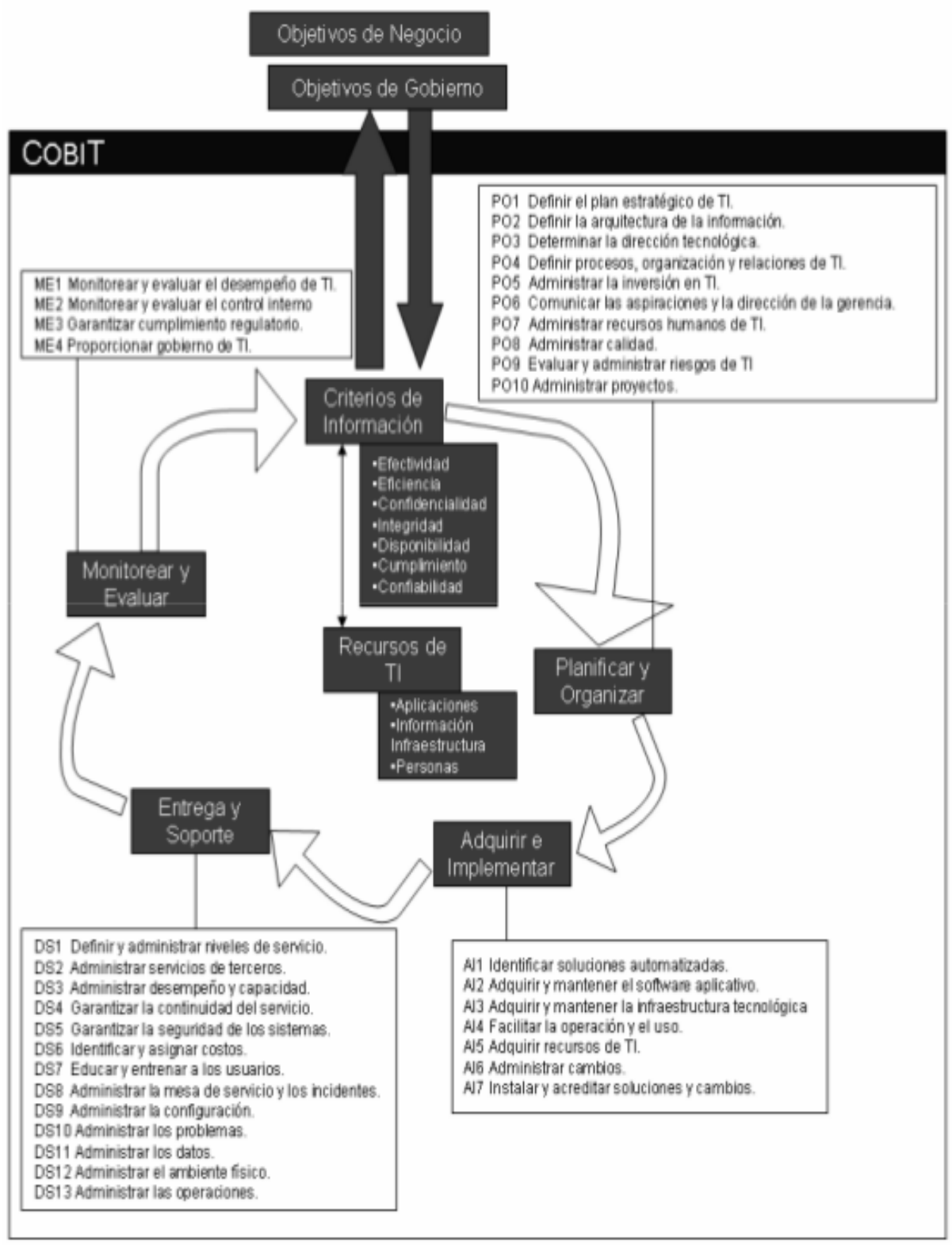


Fuente: IT Governance Institute. COBIT v.4.1

Impulsado por mediciones: La obtención de una visión objetiva del nivel de desempeño propio de una empresa no es sencilla. ¿Qué se debe medir y cómo? Las empresas deben medir dónde se encuentran y dónde se requieren mejoras, e implementar un juego de herramientas gerenciales para monitorear esta mejora (COBIT, 2007, p. 17).

- **Marco de trabajo completo de COBIT**

Gráfico 5: Marco de trabajo completo de COBIT



Fuente: IT Governance Institute. COBIT v.4.1

b) COSO II

El denominado "Informe COSO", publicado en Estados Unidos en 1992, surgió como respuesta a las inquietudes que planteaba la diversidad de conceptos, definiciones e interpretaciones existentes en torno al control interno. El Informe COSO plasma los resultados de la tarea realizada durante más de cinco años por el grupo de trabajo que la Treadway Commission, National Commission on Fraudulent Financial Reporting, creó en Estados Unidos en 1985 bajo la sigla COSO (Committee of Sponsoring Organizations) (Fernández Menta, 2003, p. 1).

- **Objetivos del COSO**

El objetivo prioritario del Informe COSO es ayudar a las organizaciones a mejorar el control de sus actividades, estableciendo un marco para los conceptos de control interno que permita una definición común de control interno y la identificación de sus componentes.

Ante la necesidad detectada de mejorar la gestión del riesgo en las organizaciones, el Comité desarrolló recientemente un nuevo marco de gestión de riesgos, titulado Enterprise Risk Management Framework. Este marco detalla los componentes esenciales de la gestión de riesgos en la empresa y el contexto en que tales componentes son eficazmente implementados.

En este trabajo se incorpora el concepto de gestión de riesgos, entendiéndose como tal un proceso, llevado a cabo por el directorio, los gerentes y el resto del personal, destinado a establecer estrategias para toda la empresa, diseñado para identificar eventos potenciales que pudieran afectar a la entidad, y administrar los riesgos para que estén dentro de los límites de su disposición al riesgo, a fin de proporcionar una razonable seguridad respecto al logro de los objetivos de la organización (Fernández Menta, 2003, p. 1).

c) Normas ISO 27000

Las normas ISO/IEC 27000 constituyen una familia de estándares, desarrolladas por la International Organization for Standardization (ISO) y por la International Electrotechnical Commission (IEC). Esta familia de estándares se publicó ante la necesidad de contar con una base para la gestión de la seguridad de la información,

especificando los requisitos para establecer, implementar, controlar, mantener e innovar un Sistema de Gestión de Seguridad de la Información (SGSI). La serie ISO 27000 está formada por varias normas. Son consideradas como normas base: ISO 27002 e ISO 27002, mientras que las normas complementarias son principalmente: ISO 27003, ISO 27004, e ISO 27005 (Quintuña, 2012, p.35).

Específicamente se ha escogido la norma ISO 27002 ya que provee las directrices adecuadas para la aplicación de esta práctica.

- **Norma ISO 27002**

La norma/estándar UNE ISO/IEC 27002 del "Sistema de Gestión de la Seguridad de la Información" es la solución de mejora continua más adecuada para evaluar los riesgos físicos (incendios, inundaciones, sabotajes, vandalismos, accesos indebidos e indeseados) y lógicos (virus informáticos, ataques de intrusión o denegación de servicios) y establecer las estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información (Fernández, 2012, p. 41).

La norma ISO 27002 está orientada al tratamiento de la seguridad de la información mediante la gestión del riesgo, tanto para sus activos como para sus procesos; esto garantiza que ante recursos limitados las inversiones sean bien focalizadas, para lograr ello se necesita de la concientización de la compañía ya que es un pilar fundamental de esta norma, por lo cual las organizaciones deben ingeniosamente buscar y adoptar mecanismos que permitan que se despierte un interés y compromiso por parte de todos los empleados (Aranda, 2009, p.2).

- **Dominios de la norma ISO 27002:2005**

Los objetivos de seguridad pueden variar considerablemente dependiendo del sector en el que se encuentre la organización, pero de forma general estos objetivos están directamente ligados a la seguridad de procesos organizativos, procesos de producción, al ciclo de vida de la información y obviamente, al cumplimiento de la legislación vigente.

Gráfico 6: Gestión de riesgos ISO 27002

Fuente: http://www.tcpsi.com/vermas/ISO_27002.htm

2.2.4 Aspecto técnico

a) Software

El soporte lógico o software de un ordenador es el conjunto de programas que permiten realizar las tareas asignadas a la máquina. En este concepto incluimos, tanto los programas suministrados en el momento de adquisición del ordenador, como los adquiridos a empresas de desarrollo y venta de programas y los escritos por los propios usuarios (LISITT, 2002, p.45).

- **Clasificación**

Cuadro 2: Clasificación del software

TIPO	DESCRIPCIÓN
Sistema operativo	Es el conjunto de programas y datos que permiten reconocer, identificar y utilizar los dispositivos de una computadora. Generalmente, los otros tipos de programas se comunican con el sistema operativo, y es éste el que comunica las órdenes a los periféricos.
Programas aplicativos	Es el conjunto de programas y datos que utilizan de forma genérica las capacidades de la computadora, para realizar tareas específicas. Generalmente se trata de programas comerciales como Microsoft Word, Macromedia Flash, etcétera; se caracterizan por permitir la creación de archivos autónomos de trabajo.
Sistemas de información	Es el conjunto de programas y datos que permiten utilizar las capacidades de procesamiento y almacenamiento de la computadora, con el fin de generar, manipular y divulgar información. Generalmente se trata de programas desarrollados en la misma organización, o adquiridos a terceros. Se caracterizan por no producir archivos autónomos de trabajo, sino por consumir bases de datos.

Fuente: Introducción a la programación, Felipe Ramírez

b) Hardware

Hardware es una palabra de origen inglés con la que se hace referencia a toda la parte "dura" de la informática, es decir a la maquinaria real utilizada para el procesamiento electrónico de datos (UNNE, 2004, p. 1).

- **Clasificación**

Cuadro 3: Clasificación del hardware

TIPO	DESCRIPCIÓN
Dispositivos de entrada	Son los dispositivos que permiten proporcionar a la computadora los datos a procesar o almacenar, o bien, indicarle a la computadora la ejecución de acciones.
Dispositivos de salida	Son los dispositivos que permiten comunicar resultados de procesamiento al usuario de la computadora.
Dispositivos de procesamiento	Son los dispositivos que se encargan del procesamiento de los datos.
Dispositivos de almacenamiento permanente	Son los dispositivos en los cuales podemos almacenar datos de manera persistente, es decir, que no se pierdan al momento de apagar el equipo.
Dispositivos periféricos	Son los dispositivos de salida que no forman parte de la computadora, pero que pueden conectarse a ésta para ampliar su funcionalidad.

Fuente: Introducción a la programación, Felipe Ramírez

c) Sistemas de información y comunicación

Una organización es un sistema. Sus componentes (mercadotecnia, manufactura, ventas, investigación, embarques contabilidad y personal) trabajan juntos para crear utilidades

que beneficien tanto a los empleados como a los accionistas de la compañía. Todo sistema organizacional depende en medida, de una entidad abstracta denominada sistema de información. Este sistema es el medio por el cual los datos fluyen de una persona o departamento hacia otros y pueden ser cualquier cosa, desde la comunicación interna entre los diferentes componentes de la organización y líneas telefónicas hasta sistemas de cómputo que generan reportes periódicos para varios usuarios. Los sistemas de información proporcionan servicios a todos los demás sistemas de una organización y enlazan todos sus componentes en forma tal que estos trabajen con eficiencia para alcanzar el mismo objetivo.

Los sistemas de información están formados por subsistemas que incluyen hardware, software, medios de almacenamiento de datos para archivos de base de datos. El conjunto particular de subsistemas utilizados (equipo específico, programas, archivos y procedimientos) se les denomina una aplicación de sistemas de información. De esta forma, los sistemas de información pueden tener aplicaciones en ventas, contabilidad o compras. Además un sistema de información es un conjunto de componentes interrelacionados que permiten reunir, procesar, almacena y distribuir información para apoyar la toma de decisiones y el control de una organización (Guachi, 2012, p. 34).

- **Beneficios**

Así mismo los sistemas de información también ayudan a los administradores y trabajadores:

- a analizar problemas,
- visualizar aspectos complejos,
- crear productos nuevos.

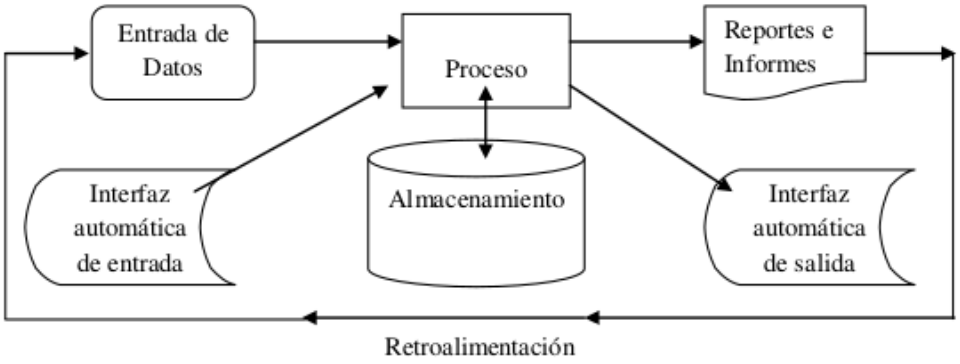
Un sistema de información produce la información que las organizaciones necesitan para:

- tomar decisiones,
- controlar operaciones,
- analizar problemas,
- crear y producir y/o servicios nuevos.

Las actividades de un sistema de información son: entrada, procesamiento y salida. La entrada captura o recolecta datos del interior de la organización o de su entorno para ser procesados en un sistema de información (Guachi, 2012, p. 35).

- **Ciclo del sistema de información**

Gráfico 7: Ciclo de un sistema de información



Fuente: Norma de seguridad informática ISO 27002 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el departamento de sistemas de la Cooperativa de ahorro y crédito San Francisco Ltda., Tania Guachi.

d) Modelo de madurez

El modelo de madurez para la administración y el control de los procesos de TI se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente (0) hasta un nivel de optimizado (5). Este enfoque se deriva del modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad del desarrollo de software. Cualquiera que sea el modelo, las escalas no deben ser demasiado granulares, ya que eso haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable debido a que en general, el fin es identificar dónde se encuentran los problemas y cómo fijar prioridades para las mejoras. El propósito no es avaluar el nivel de adherencia a los objetivos de control.

Los niveles de madurez están diseñados como perfiles de procesos de TI que una empresa reconocería como descripciones de estados posibles actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior (COBIT, 2007, p. 17).

- **Beneficios**

Utilizando los modelos de madurez desarrollados para cada uno de los 34 procesos TI de COBIT, la gerencia podrá identificar:

- El desempeño real de la empresa—Dónde se encuentra la empresa hoy
- El estatus actual de la industria—La comparación
- El objetivo de mejora de la empresa—Dónde desea estar la empresa
- El crecimiento requerido entre "como es" y "como será"

- **Modelo genérico de madurez**

Cuadro 4: Modelo genérico de madurez

0 No Existente- Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.
1 Inicial- Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.
2 Repetible- Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.
3 Definido- Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los

procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.
4 Administrado- Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.
5 Optimizado- Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

Fuente: IT Governance Institute. COBIT v.4.1

2.2.5 Marco conceptual

Administrador de sistema: Los términos administrador de red, especialista de red y analista de red se designan a aquellas posiciones laborales en las que los ingenieros se ven involucrados en redes de computadoras, o sea, las personas que se encargan de la administración de la red.

Los administradores de red son básicamente el equivalente de red de los administradores de sistemas: mantienen el hardware y software de la red (Wikipedia, 2015).

Archivo: Un archivo o fichero informático es un conjunto de bits que son almacenados en un dispositivo. Un archivo es identificado por un nombre y la descripción de la carpeta o directorio que lo contiene. A los archivos informáticos se les llama así porque son los equivalentes digitales de los archivos escritos en libros, tarjetas, libretas, papel o microfichas del entorno de oficina tradicional (Wikipedia, 2015)

Auditor: Persona capacitada y designada por parte competente, para examinar determinadas cuentas e informar o dictaminar acerca de ellas. Originalmente la palabra que se define significa “oidor” u “oyente”. El origen de su uso en la contaduría puede encontrarse en épocas remotas en Inglaterra, cuando pocas personas sabían leer y las cuentas de los grandes propietarios eran “oídas” (escuchadas) en vez de ser examinadas como en la actualidad (Secretaria de Hacienda y Crédito Público, 2005, p. 49).

Auditoría: Técnica de control, dirigida a valorar, el control interno y la observancia de las Normas Generales de Contabilidad. Comprende un examen independiente de los registros de contabilidad y otra evidencia relacionada con una entidad para apoyar la opinión experta imparcial sobre la confiabilidad de los estados financieros (MAC, 2007, p. 2).

Automatización: La automatización de tareas es, en informática, el conjunto de métodos que sirven para realizar tareas repetitivas en un ordenador. Algunos métodos para la automatización de tareas son la programación simple, los macros, los intérpretes y las bombas lógicas. También hay algunos programas específicos que automatizan tareas. Incluso los virus informáticos utilizados de forma benéfica podrían considerarse otro método para la automatización de tareas para el usuario (Wikipedia, 2014).

Cliente/servidor: Este término define la relación entre dos programas de computación en el cual uno, el cliente, solicita un servicio al otro, el servidor, que satisface el pedido (Deiviz, 2007, p. 4).

COBIT: Control Objectives for Information and related Technology. Desarrollado por Information Systems Audit and Control Association (ISACA). Centra su interés en la gobernabilidad, aseguramiento, control y auditoría para Tecnologías de la Información y Comunicación (TIC) (Quintuña, 2012, p.18).

Computadora: La computadora1 2 (del inglés: computer; y este del latín: computare, 'calcular'), también denominada computador3 1 u ordenador4 5 (del francés: ordinateur; y este del latín: ordinator), es una máquina electrónica que recibe y procesa datos para convertirlos en información conveniente y útil. Una computadora está formada, físicamente, por numerosos circuitos integrados y otros muchos componentes de apoyo, extensión y accesorios, que en conjunto pueden ejecutar tareas diversas con suma rapidez y bajo el control de un programa (Wikipedia, 2015).

Contraseña: Una contraseña o clave es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se les permite el acceso. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso (Wikipedia, 2015).

Control: Actividad dirigida a verificar el cumplimiento de los planes, programas, políticas, normas y procedimientos, a fin de detectar desviaciones e identificar posibles acciones correctivas (Zambrano, 2012, p.36).

Cortafuegos: Un cortafuegos (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios (Wikipedia, 2015).

COSO: Committee of Sponsoring Organizations. Hace recomendaciones a los administradores de TI sobre cómo evaluar, informar e implementar sistemas de control, teniendo como objetivo la efectividad y eficiencia de las operaciones, la información financiera y el cumplimiento de las regulaciones, valoración de riesgos, actividades de control, información y comunicación y la verificación (Quintuña, 2012, p.19).

Datos: Un dato es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa. Los datos describen hechos empíricos, sucesos y entidades. Es un valor o referente que recibe el computador por diferentes medios, los datos representan la información que el programador manipula en la construcción de una solución o en el desarrollo de un algoritmo (Wikipedia, 2015).

Dictamen: Opinión, consejo, o juicio que en determinados asuntos debe oírse, por los tribunales, corporaciones o entes públicos. También se llama así, al informe u opinión verbal o por escrito que expone un letrado, a petición del cliente, acerca de un problema jurídico o sometido a su consideración (Zambrano, 2012, p.42).

Dominio: Un dominio puede referirse a dos cosas: es un conjunto de ordenadores conectados en una red que confían a uno de los equipos de dicha red, la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en dicha red; o es la parte principal de una dirección en la web que indica la organización o compañía que administra dicha página (Wikipedia, 2015).

Empresa: Unidad productora de bienes y servicios homogéneos para lo cual organiza y combina el uso de factores (Secretaria de Hacienda y Crédito Público, 2005, p. 170).

Estándar: Un estándar es un conjunto de reglas que deben cumplir los productos, procedimientos o investigaciones que afirmen ser compatibles con el mismo producto. Los estándares ofrecen muchos beneficios, reduciendo las diferencias entre los productos y generando un ambiente de estabilidad, madurez y calidad en beneficio de consumidores e inversores (Hernández, 2011, p.69).

Evidencia: Las pruebas que obtiene el auditor durante la ejecución de la auditoría, que hace patente y manifiesta la certeza o convicción sobre los hechos o hallazgos que prueban y demuestran claramente éstos, con el objetivo de fundamentar y respaldar sus opiniones y conclusiones (Miyar, 2007, p. 3).

Información: La información es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje (Wikipedia, 2015).

Informática: La informática, también llamada computación en América, es una ciencia que estudia métodos, procesos, técnicas, con el fin de almacenar, procesar y transmitir información y datos en formato digital (Wikipedia, 2015).

Infraestructura: La tecnología, los recursos humanos y las instalaciones que permiten el procesamiento de las aplicaciones (COBIT, 2007, p. 190).

ISO: International Organization for Standardization. Integra un conjunto de normas sobre Sistemas de Gestión de Seguridad de la Información (SGSI), que a través de su aplicación, permite administrar la información mediante el modelo Plan – Do – Check – Act (PDCA) (Quintuña, 2012, p.19).

ITIL: Librería de Infraestructura de TI de la Oficina de Gobierno Gubernamental del Reino Unido (OGC). Un conjunto de lineamientos sobre la administración y procuración de servicios operativos de TI (COBIT, 2007, p. 190).

Outsourcing: El término de externalización (No reconocido por el Diccionario de la RAE) proviene de la traducción al castellano del neologismo inglés outsourcing. Es el proceso en el cual una empresa delega una porción de su proceso de negocio a una compañía externa (Wikipedia, 2014).

Patrimonio: El patrimonio es el conjunto de bienes y derechos, cargas y obligaciones, pertenecientes a una persona, física o jurídica (Wikipedia, 2014).

Periférico: Se considera periférico al conjunto de dispositivos que sin pertenecer al núcleo fundamental de la computadora, formado por la Unidad central de procesamiento (CPU) y la memoria central, permitan realizar operaciones de entrada/salida (E/S) complementarias al proceso de datos que realiza la CPU (Wikipedia, 2014).

Red Informática: Una red de computadoras, también llamada red de ordenadores, red de comunicaciones de datos o red informática, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios (Wikipedia, 2015).

Retroalimentación: Es un mecanismo por el cual una cierta proporción de la salida de un sistema se redirige a la entrada, con objeto de controlar su comportamiento.1 La realimentación se produce cuando las salidas del sistema o la influencia de las salidas del sistemas en el contexto, vuelven a ingresar al sistema como recursos o información. La realimentación permite el control de un sistema y que el mismo tome medidas de corrección con base en la información realimentada (Wikipedia, 2015).

Riesgo: El riesgo de que una amenaza específica explote las debilidades de un activo o grupo de activos para ocasionar pérdida y/o daño a los activos. Por lo general se mide por medio de una combinación del impacto y la probabilidad de ocurrencia (COBIT, 2007, p. 191).

Sabotaje: El sabotaje (del francés sabotage, 'fabricar zapatos; colocar rieles; sabotear') es un proceso por el cual se realiza una modificación, destrucción, obstrucción o cualquier intervención en una operación ajena, con el propósito de obtener algún beneficio para uno mismo (Wikipedia, 2014).

Seguridad: La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable (Wikipedia, 2015).

Servidor: computadora central de un sistema de red que provee servicios y programas a otras computadoras conectadas (Deiviz, 2007, p. 17).

TI: Tecnología de información (COBIT, 2007, p. 192).

Usuario: Una persona que utiliza los sistemas empresariales (COBIT, 2007, p. 192).

Vandalismo: El concepto de vandalismo es un concepto que tiene que ver con la convivencia en sociedad y que se aplica para designar a aquellos actos de extrema violencia que suponen agresiones especialmente contra mobiliario o inmobiliario que puede ser propio o no (COBIT, 2007, p. 192).

2.3 HIPÓTESIS

2.3.1 Hipótesis general

- La elaboración de una auditoría de sistemas informáticos en la Cooperativa de Ahorro y Crédito “Educadores de Chimborazo” Ltda., de la ciudad de Riobamba, provincia de Chimborazo para el período 2014 permitirá dictaminar respecto a la economía, eficiencia y eficacia de la utilización de los recursos tecnológicos.

2.3.2 Hipótesis específicas

- El estructurar un marco teórico referencial contribuirá al desarrollo de la presente investigación.

- La aplicación de la norma COBIT 4.1 y la norma ISO 27002, permitirá detectar la existencia de vulnerabilidades en los recursos de tecnologías de la información.

- La emisión de un informe mostrando las respectivas conclusiones y recomendaciones ayudará a la gerencia y al personal a tomar los correctivos pertinentes.

2.4 VARIABLES

2.4.1 Variable Independiente

- Auditoría de sistemas informáticos.

2.4.2 Variable Dependiente

- Economía, eficiencia y eficacia de la utilización de los recursos tecnológicos.

CAPÍTULO III: MARCO METODOLÓGICO

3.1 MODALIDAD

a) Cualitativa – Cuantitativa

Según Bernal una investigación es cuantitativa cuando se fundamenta en la medición de las características de los fenómenos sociales, lo cual supone derivar de un marco conceptual pertinente al problema analizado, una serie de postulados que expresen relaciones entre las variables estudiadas de forma deductiva. Este método tiende a generalizar y normalizar resultados.; y cualitativa (citando a Bonilla y Rodríguez (2000)), se orienta a profundizar casos específicos y no a generalizar. Su preocupación no es prioritariamente medir, sino cualificar y describir el fenómeno social a partir de rasgos determinantes, según sean percibidos por los elementos mismos que están dentro de la situación estudiada (2006, p.60).

3.2 TIPOS DE INVESTIGACIÓN

a) Aplicada

Este tipo de investigación también recibe el nombre de práctica, activa, dinámica. Se caracteriza porque busca la aplicación o utilización de los conocimientos que se adquieren (Behar, 2008, p. 20).

b) Bibliográfica – Documental

Este tipo de investigación es la que se realiza, como su nombre lo indica, apoyándose en fuentes de carácter documental, esto es, en documentos de cualquier especie. Como subtipos de esta investigación encontramos la investigación bibliográfica, la hemerográfica y la archivística; la primera se basa en la consulta de libros, la segunda en artículos o ensayos de revistas y periódicos y la tercera en documentos que se encuentran en los archivos, como cartas, oficios, circulares, expedientes, etcétera (Behar, 2008, p. 20).

c) De campo

Este tipo de investigación se apoya en informaciones que provienen entre otras, de entrevistas, cuestionarios, encuestas y observaciones. Como es compatible desarrollar este tipo de investigación junto a la investigación de carácter documental, se recomienda que primero se consulten las fuentes de la de carácter documental, a fin de evitar una duplicidad de trabajos (Behar, 2008, p. 21).

d) Investigación descriptiva

Mediante este tipo de investigación, que utiliza el método de análisis, se logra caracterizar un objeto de estudio o una situación concreta, señalar sus características y propiedades. Combinada con ciertos criterios de clasificación sirve para ordenar, agrupar o sistematizar los objetos involucrados en el trabajo indagatorio. Al igual que la investigación que hemos descrito anteriormente, puede servir de base para investigaciones que requieran un mayor nivel de profundidad. Su objetivo es describir la estructura de los fenómenos y su dinámica, identificar aspectos relevantes de la realidad (Behar, 2008, p. 21).

3.3 POBLACIÓN Y MUESTRA

En el presente trabajo se efectuará en el cantón Riobamba, provincia de Chimborazo.

Población: La población que se tomará para realizar la presente investigación corresponde al total de empleados que laboran en la Cooperativa y por tanto utilizan directa o indirectamente los distintos equipos informáticos, la misma que corresponde a 16 personas.

Muestra: En este caso el cálculo de la muestra para el estudio no aplica ya que la población antes mencionada es manejable para el desarrollo del presente trabajo de revisión.

3.4 MÉTODOS, TÉCNICAS E INSTRUMENTOS

3.4.1 Métodos

a) Método investigación - acción

El objetivo de este método está en producir los cambios en la realidad estudiada. Por medio de este método nos preocuparemos por resolver los problemas específicos utilizando una metodología rigurosa. El objetivo de la utilización de este método es situarse en un contexto espaciotemporal, intencionalmente unido a la realidad de cada día que se origina a partir de la experiencia vivida.

Para COHEN y MANION este tipo de investigación es adecuada siempre que se requiera un conocimiento específico para un problema específico en una situación específica. Dentro de las opciones metodológicas de este método esta la adaptación de la metodología cuantitativa (incluyendo la experimentación, control de variables, análisis estadístico, etc.) y la posibilidad de contemplarse como una extensión lógica del concepto de "praxis". Este postulado plantea que el criterio de la verdad solo puede ser la práctica social (Behar, 2008, p. 42).

b) Método inductivo

El método inductivo crea leyes a partir de la observación de los hechos, mediante la generalización del comportamiento observado; en realidad, lo que realiza es una especie de generalización, sin que por medio de la lógica pueda conseguir una demostración de las citadas leyes o conjunto de conclusiones.

Dichas conclusiones podrían ser falsas y, al mismo tiempo, la aplicación parcial efectuada de la lógica podría mantener su validez; por eso, el método inductivo necesita una condición adicional, su aplicación se considera válida mientras no se encuentre ningún caso que no cumpla el modelo propuesto. (Behar, 2008, p. 42).

c) Método hipotético-deductivo

En el método hipotético-deductivo (o de contrastación de hipótesis) se trata de establecer la verdad o falsedad de las hipótesis (que no podemos comprobar directamente, por su carácter de enunciados generales, o sea leyes, que incluyen términos teóricos), a partir de la verdad o falsedad de las consecuencias observacionales, unos enunciados que se refieren a objetos y propiedades observables, que se obtienen deduciéndolos de las hipótesis y, cuya verdad o falsedad estamos en condiciones de establecer directamente.

La esencia del método hipotético-deductivo consiste en saber cómo la verdad o falsedad del enunciado básico dice acerca de la verdad o la falsedad de la hipótesis que ponemos a prueba. Por supuesto, el proceso puede ser mucho más largo, e incluir hipótesis intermedias (Behar, 2008, p. 40).

3.4.2 Técnicas

a) Examen

El auditor aplica esta herramienta con el propósito de investigar algún hecho, comprobar alguna cosa, verificar la forma de realizar un proceso, evaluar la aplicación de las técnicas, métodos y procedimientos de trabajo, verificar el resultado de una transacción, comprobar la operación correcta de un sistema computacional y para evaluar muchos otros aspectos.

Dentro del ambiente de la auditoría de sistemas computacionales, esta herramienta se utiliza, entre muchas cosas, para inspeccionar la operación correcta del sistema, analizar el desarrollo adecuado de los proyectos informáticos, examinar la forma en que se realiza la captura y el procesamiento de datos, así como la emisión de resultados; también se emplea para inspeccionar las medidas de seguridad del sistema y del área de informática, examinar el acceso a dicha área, al sistema, a sus programas y a la información de las bases de datos, para examinar la forma en que se archivan y protegen los datos de los sistemas, sus programas y la propia información; además pone a prueba el cumplimiento de las funciones y actividades de los funcionarios, personal y usuarios del centro de cómputo (Muñoz Razo, 2002, pp. 418-419).

b) Inspección

La técnica de inspección está relacionada con la aplicación de los exámenes que se realizan para evaluar el funcionamiento de dichos sistemas; mediante la inspección se evalúa la eficiencia y eficacia del sistema, en cuanto a operación y procesamiento de datos. Lo mismo ocurre para la gestión administrativa de un centro de cómputo, en donde se hace una inspección detallada con el propósito de evaluar el cumplimiento de sus funciones, actividades, estructura organizacional y todos los demás aspectos administrativos.

La inspección se realiza a cualquiera de las actividades, operaciones y componentes que rodean los sistemas. Con esta técnica se puede evaluar, verificar y juzgar el funcionamiento de los sistemas computacionales de la empresa, así como la realización adecuada de todas sus actividades (Muñoz Razo, 2002, p. 425).

c) Confirmación

La absoluta confianza en las opiniones emitidas en el dictamen de la auditoría es uno de los aspectos fundamentales de esta disciplina, debido a que los resultados deben estar fundamentados en información que sea plenamente comprobada y confirmada a través del uso de las técnicas, herramientas, procedimientos e instrumentos adecuados para la auditoría.

La característica fundamental de una auditoría, cualquiera que sea su tipo, es la autenticidad con la que el auditor emite sus opiniones, sean a favor o en contra.

Debemos reiterar que en la auditoría de sistemas computacionales, al igual que en otras auditorías, la confirmación es uno de los elementos fundamentales que ayudan al auditor a certificar la validez de su dictamen de auditoría (Muñoz Razo, 2002, p. 427).

d) Comparación

La utilidad de esta herramienta radica en que permite hacer la evaluación de datos similares o iguales entre dos entidades (la analizada y una similar); con esto se obtiene información relevante para la evaluación de la entidad evaluada, ya que se compara la forma en que debería funcionar y la forma en que está funcionando, en relación con la otra entidad (Muñoz Razo, 2002, p. 428).

e) Revisión documental

En esta evaluación se revisan los manuales, instructivos, procedimientos diseñados para las funciones, actividades y operaciones, el registro de resultados, estadísticas y otros instrumentos de registro formal de los alcances obtenidos, la interpretación de los acuerdos, memorandos, normas, políticas y todos los aspectos formales que se asientan por escrito para el cumplimiento de las funciones y actividades en la administración cotidiana de las empresas (Muñoz Razo, 2002, p. 430).

f) Matriz FODA o DOFA

Por medio de este documento se puede tener una apreciación preliminar sobre las fortalezas y debilidades del propio centro de información de la empresa, y se pueden analizar sus posibles amenazas y áreas de oportunidad; con dicho análisis, el auditor evalúa el cumplimiento de la misión y objetivo general del área de sistemas computacionales de la empresa.

La matriz DOFA es un acrónimo de Debilidades, Oportunidades, Fortalezas y Amenazas de la empresa, las cuales se estudian cada una por separado en cuanto a su presencia interna y a la influencia que la empresa recibe del exterior, y conforme a los siguientes criterios: (Muñoz Razo, 2002, p. 454).

Gráfico 8: Funcionamiento matriz DOFA

Fuente: Auditoría de sistemas computacionales, Carlos Muñoz Razo

3.4.3 Instrumentos

a) El cuestionario

Es la recopilación de datos mediante preguntas impresas en cédulas o fichas, en las que el encuestado responde de acuerdo con su criterio; de esta manera, el auditor obtiene información útil que puede concentrar, clasificar e interpretar por medio de su tabulación y análisis, para evaluar lo que está auditando y emitir una opinión sobre el aspecto investigado.

El cuestionario tiene la gran ventaja de que puede recopilar una gran cantidad de información, debido a que contiene preguntas sencillas cuyas respuestas no implican ninguna dificultad; además, como en otros métodos, su aplicación es de carácter impersonal y libre de influencias y compromisos para el entrevistado. También tiene la ventaja de poder seleccionar los tipos de preguntas que se deben realizar, los cuales señalaremos a continuación (Muñoz Razo, 2002, p. 340).

b) La entrevista

La entrevista podría entenderse como la recopilación de información que se realiza en forma directa, cara a cara y a través de algún medio de captura de datos, es decir, el auditor interroga, investiga y confirma directamente con el entrevistado sobre los aspectos que está auditando; en la aplicación de esta técnica, el auditor utiliza una guía de entrevista, la cual contiene una serie de preguntas preconcebidas que va adaptando conforme recibe la información del entrevistado, de acuerdo con las circunstancias que se le presentan y en busca de obtener más información útil para su trabajo (Muñoz Razo, 2002, p. 329).

c) La encuesta

Es la recopilación de datos concretos sobre un tema específico, mediante el uso de cuestionarios o entrevistas diseñados con preguntas precisas para obtener las opiniones de los encuestados, las cuales permiten, después de hacer una rápida tabulación, análisis

e interpretación de esa información, conocer su punto de vista y sentimientos hacia un tópico específico (Muñoz Razo, 2002, p. 348).

d) La observación

Es el hecho de examinar, analizar, advertir o estudiar algo; en este caso, cuando el auditor de sistemas aplica esta técnica, lo que hace es observar todo lo relacionado con los sistemas de una empresa, con el propósito de percibir, examinar o analizar lo relacionado con los eventos que se presentan en el desarrollo de las actividades de un sistema, de un centro de sistematización, de la operación de la computadora o el desempeño de cualquiera de las actividades que le permitirán evaluar el cumplimiento de las operaciones del sistema (Muñoz Razo, 2002, p. 360).

e) Inventarios

Esta forma de recopilación de información consiste en hacer un recuento físico de lo que se está auditando, a fin de saber la cantidad existente de algún producto en una fecha determinada y compararla con la que debería haber según los documentos en esa misma fecha. Consiste propiamente en comparar las cantidades reales existentes con las que debería haber para comprobar que sean iguales o, en caso contrario, para resaltar las posibles diferencias e investigar sus causas (Muñoz Razo, 2002, p. 367).

f) La experimentación

Es la observación de un fenómeno en estudio, al cual se le van adaptando o modificando sus variables conforme a un plan predeterminado, con el propósito de analizar sus posibles cambios de conducta como respuesta a las modificaciones que sufre dentro de su propio ambiente o en un ambiente ajeno.

Todo ello con el fin de estudiar su comportamiento bajo diversas circunstancias y sacar conclusiones. (Muñoz Razo, 2002, p. 410).

3.5 RESULTADOS

De acuerdo al resultado obtenido se puede comprobar que el chi-cuadrado es mayor que el chi-cuadrado tabla ($\boldsymbol{X^2C > X^2t = 12,80 > 3,84}$) por lo que se acepta la hipótesis de trabajo y se rechaza la hipótesis nula; es decir que se ha comprobado que "La aplicación de una Auditoría Informática dentro de la Cooperativa de Ahorro y Crédito Educadores de Chimborazo Ltda., de la ciudad de Riobamba, Provincia de Chimborazo para el período 2014 permitirá conocer el nivel de eficiencia, eficacia y economía en la utilización de los recursos tecnológicos"; esto demuestra que la variable dependiente está ligada a la variable independiente.

3.6 VERIFICACIÓN DE HIPÓTESIS O IDEA A DEFENDER

Cuadro 5: Verificación de la hipótesis

RESPUESTAS / PREGUNTAS	SI	NO	TOTAL
VARIABLE INDEPENDIENTE			
¿Sus claves de acceso al sistema son conocidas única y exclusivamente por usted?	11	0	11
¿Conoce usted los métodos para establecer claves seguras?	4	7	11
¿Le han indicado que hacer en caso de olvido o pérdida de sus claves?	11	0	11
¿Cree que existen las seguridades adecuadas para evitar daños o alteraciones en los sistemas de la cooperativa?	11	0	11
Total Variable Independiente	**37**	**7**	**44**
VARIABLE DEPENDIENTE			
¿Ha tenido fallos del equipo informático mientras trabaja en él?	0	11	11
¿Comunica usted de forma breve al departamento de sistemas cuando tiene problemas con los equipos?	11	0	11
¿El departamento de sistemas atiende sus requerimientos de forma oportuna?	11	0	11
¿Conoce usted el procedimiento adecuado para eliminar archivos de su equipo para evitar el mal uso de la información ahí contenida?	11	0	11
¿Se le ha entregado manuales de procedimientos o políticas de manejo de los equipos por escrito?	0	11	11
¿Considera usted qué el equipo que usa satisface los requerimientos necesarios para el desempeño de sus labores?	11	0	11
¿Conoce usted las políticas generales para el uso y operación de los equipos informáticos?	0	11	11
¿Conoce usted las políticas que se han establecido para el	0	11	11

cambio de claves de acceso al sistema operativo, correo electrónico, otros sistemas?			
¿Crea usted respaldos de la información y demás archivos con los que trabaja?	3	8	11
¿Guarda sus respaldos en un lugar seguro?	3	8	11
¿Cree usted que la información interna de la cooperativa está bien resguardada?	11	0	11
¿Cree usted que los equipos de la cooperativa están bien resguardados?	11	0	11
Total Variable Dependiente	**72**	**60**	**132**
TOTAL	**109**	**67**	**176**

Fuente: Investigación
Realizado por: Autor

Verificación de hipótesis

Con la finalidad de comprobar la hipótesis establecida en la presente investigación se ha utilizado la prueba estadística del Chi-cuadrado, este método ayuda a determinar si las dos variables están relacionadas o no y permite la aceptación o rechazo de la hipótesis que se relata en el estudio.

Para la verificación de la hipótesis es necesario aplicar los siguientes pasos:

Formulación de las Hipótesis

- **Hipótesis Nula (H0)**: "La aplicación de una Auditoría Informática dentro de la Cooperativa de Ahorro y Crédito de Educadores de Chimborazo Ltda., de la ciudad de Riobamba, Provincia de Chimborazo para el Período 2014 no permitirá conocer el nivel de eficiencia, eficacia y economía en la utilización de los recursos tecnológicos".

- **Hipótesis de Trabajo (H1):** "La aplicación de una Auditoría Informática dentro de la Cooperativa de Ahorro y Crédito de Educadores de Chimborazo Ltda., de la ciudad de Riobamba, Provincia de Chimborazo para el Período 2014 permitirá conocer el nivel de eficiencia, eficacia y economía en la utilización de los recursos tecnológicos".

Matriz de Contingencia

Los datos utilizados en esta tabla han sido obtenidos de la tabulación de las encuestas.

Cuadro 6: Matriz de contingencia

RESPUESTAS (x) / VARIABLES (y)	SI	NO	TOTAL
Independiente	37	7	44
Dependiente	72	60	132
TOTAL	**109**	**67**	**176**

Fuente: Investigación
Realizado por: Autor

Hallar la Frecuencia Esperada (E)

En este punto es necesario aplicar la siguiente fórmula:

$$E = \frac{TF * TC}{TG}$$

Dónde:

E= Frecuencia esperada

TF= Total de cada fila

TC= Total de cada columna

$E_1 = \frac{44*109}{176} = \mathbf{27}$

$E_2 = \frac{44*67}{176} = \mathbf{17}$

$E_3 = \frac{132*109}{176} = \mathbf{82}$

$E_4 = \frac{132*67}{176} = \mathbf{50}$

Hallar el Chi-cuadrado Tabla (X2t)

Para la identificación de la chi-cuadrado tabla se debe determinar el grado de libertar y el nivel de confianza, posterior a ello se escogerá el valor correspondiente de acuerdo al cálculo realizado.

GL = (F-1) (C-1)

GL = (2-1) (2-1) = 1

Donde:

GL= Grados de libertad

F= Fila

Chi - Cuadrado

Cuadro 7: Chi cuadrado

Alfa / Grados de libertad	0,1	0,05	0,025	0,01	0,005
1	2,71	3,84	5,02	6,63	7,88
2	4,61	5,99	7,38	9,21	10,60

Fuente: Investigación
Realizado por: Autor

Alfa: Este valor hace referencia al nivel de confianza que deseamos que tengan los cálculos de la prueba; en este caso el nivel de confianza es del 95%, el valor de alfa debe ser del 0,05 lo cual corresponde al complemento porcentual de la confianza. Entonces Chi-cuadrado tabla (X2t)= 3,84.

Hallar el Chi-cuadrado

La fórmula es la siguiente:

$$X^2C = \sum \frac{(O-E)^2}{E}$$

Donde:

X^2C = Chi–cuadrado

$\sum$ = Sumatoria

O = Frecuencia observada

Chi-cuadrado calculado

Cuadro 8: Chi cuadrado calculado

CASILLAS (X, Y)	O	E	$\frac{(O-E)^2}{E}$
Si variable independiente	37	27	3,70
No variable independiente	7	17	5,88
Si variable dependiente	72	82	1,22
No variable dependiente	60	50	2,00
$X^2C = \sum \frac{(O-E)^2}{E}$			**= 12,80**

Fuente: Investigación
Realizado por: Autor

Decisión:

Para la toma de la decisión correspondiente es importante recordar que:

$$X^2C > X^2t = Hipótesis\ de\ trabajo$$

$$X^2C < X^2t = Hipótesis\ nula$$

CAPÍTULO IV: MARCO PROPOSITIVO

4.1 TÍTULO

"AUDITORÍA DE SISTEMAS INFORMÁTICOS EN LA COOPERATIVA DE AHORRO Y CRÉDITO EDUCADORES DE CHIMBORAZO LTDA., DE LA CIUDAD DE RIOBAMBA, PROVINCIA DE CHIMBORAZO PARA EL PERÍODO 2014."

4.2 CONTENIDO DE LA PROPUESTA

4.2.1 Metodología, guía y/o procedimiento

FASE I: Planeación de la auditoría.

FASE II: Ejecución de la Auditoría.

FASE III: Informe de la Auditoría.

4.2.2 Implementación de la propuesta

4.2.2.1 Planeación de la auditoría

Cuadro 9: Datos generales de la CACECH

INSTITUCIÓN:	COOPERATIVA DE AHORRO Y CRÉDITO EDUCADORES DE CHIMBORAZO LTDA.
DIRECCIÓN:	José Veloz 22 – 11 y Eugenio Espejo (Esquina)
NATURALEZA DEL TRABAJO:	Auditoría de Sistemas Informáticos
PERÍODO:	Año 2014

Fuente: Información CACECH

4.2.2.1.1 Identificar el origen del trabajo

El presente trabajo a desarrollarse entra dentro de una catalogación especial, ya que el motivo principal de su realización es que sirva como requisito al evaluador para la obtención de su título profesional, y, para la organización dentro de su programa integral de auditoría ya que sus demás áreas han sido evaluadas con anterioridad, faltándole solo la parte de los sistemas informáticos para que pueda tener un panorama de su situación actual general.

4.2.2.1.2 Hoja de índices y marcas

	HOJA DE ÍNDICES Y MARCAS	IM 1/2
MARCA	**SIGNIFICADO**	
✓	Verificado	
✓✓	Dato correcto	
☑	Verificado dos veces	
	Cotejado con documentos	
	Cotejado con inventario	
×	Dato con error	
©	Pendiente de chequear	
¿?	Confirmar preguntas	
‖	Observación importante	
	Listado de resultados	
	Comentario especial	
	Observación	
☒	No coinciden los datos	
PSL	Programa de Auditoría Seguridad Lógica	
PSF	Programa de Auditoría Seguridad Física	
PTC	Programa de Auditoría Tecnologías de la Información y Comunicación	
PGI	Programa de Auditoría Gestión Informática	
CCI	Cuestionario de Control Interno	
AF	Análisis FODA	
HH	Hoja de hallazgos	
IM	Hoja de índices y marcas	
DP	Datos Preliminares	
PS	Propuesta de Servicios Profesionales	
OT	Orden de Trabajo	
CC	Carta Compromiso	
Elaborado por: EGMA	**Fecha:** 2015-08-08	
Revisado por: VSHB	**Fecha:** 2015-08-08	

	HOJA DE ÍNDICES Y MARCAS	IM 2/2

MARCA	SIGNIFICADO
CT	Contrato de Trabajo
NI	Notificación de Inicio de la Auditoría
PGA	Programa General de Auditoría
CCI	Cuestionario de Control Interno
PA	Presupuesto General
IF	Informe Final
EGMA	Erazo Granizo Michael Adrián
VSHB	Veloz Segovia Hítalo Bolívar
PO	Planear y Organizar
AI	Adquirir e Implementar
DS	Entregar y Dar Soporte
ME	Monitorear y Evaluar
CACECH	Cooperativa de Ahorro y Crédito "Educadores de Chimborazo Ltda."
✓	Realizado/Seleccionado
x	Selección dominio
⊙	Selección subdominio

Elaborado por: EGMA	**Fecha:** 2015-08-08
Revisado por: VSHB	**Fecha:** 2015-08-08

4.2.2.1.3 Programa general de auditoría

	PROGRAMA GENERAL DE AUDITORÍA	**PGA**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

Objetivos

General:

- ✓ Evaluar la efectividad de los procesos claves referentes a los sistemas informáticos, utilizando como criterios de comparación las normas COBIT 4.1 y las Normas ISO 27002.

Específicos:

- ✓ Determinar si existe un manejo adecuado de los equipos informáticos de la entidad a fin de asegurar economía y fiabilidad en los resultados que los mismos emiten.
- ✓ Comprobar una seguridad razonable de los recursos para verificar empatía entre los objetivos de control y los objetivos generales del negocio.
- ✓ Verificar el nivel actual del control interno de la entidad para determinar su nivel actual y cuantificarlo de acuerdo a una escala establecida por COBIT 4.1.
- ✓ Consultar respecto a los sistemas informáticos y los sistemas de comunicaciones para determinar debilidades y fortalezas de los mismos.
- ✓ Presentar de un informe para dar a conocer los resultados, conclusiones y recomendaciones.

N.	PROCEDIMIENTO	REF. P/T	ELAB. POR	FECHA	OBSERVACIONES
1	Realice el levantamiento de la información	**DP**	**EGMA**	2015-08-10	---
2	Realice la Propuesta de Servicios Profesionales	**PS**	**EGMA**	2015-08-10	---
3	Elabore la carta de notificación de inicio de la auditoría	**CC**	**EGMA**	2015-08-13	---
4	Ejecute auditoría	**OT**	**EGMA**	2015-09-13	---
5	Elabore borrador del informe para revisión	**CT**	**EGMA**	2015-10-14	---
6	Redacte el informe final	**NI**	**EGMA**	2015-10-15	---
7	Presente informe con respectivos comentarios y sugerencias.	**IF**	**EGMA**	2015-10-23	---
Elaborado por: **EGMA**			**Fecha:** 2015-08-08		
Revisado por: **VSHB**			**Fecha:** 2015-08-08		

	INFORMACIÓN GENERAL	**DP 1/6**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

ANTECEDENTES

La Cooperativa de Ahorro y Crédito Educadores de Chimborazo, CACECH; fundada el 26 de Junio de 1964; es una Institución financiera Cooperativista de carácter gremial cerrado; sus más de 3300 socios pertenecen al Magisterio de la provincia de Chimborazo, quienes al hacer sus aportaciones mensuales, practican el principio fundamental del Cooperativismo... la solidaridad.

La CACECH, se encuentre ubicada en el centro histórico la ciudad de Riobamba, capital de la provincia de Chimborazo, en las calles Veloz y Espejo; su edificación de corte colonial, brinda un ambiente acogedor para sus socios quienes pueden acercarse a sus instalaciones en horario de 09:00 a 12:00 y de 14:00 a 19:00, en donde serán atendidos con la calidad y calidez propias de su talento humano.

Entre sus principales productos financieros podemos mencionar: Libretas de Libre Ahorro – Libre Retiro; Libreta de Ahorro Cautivo y Fondos de Reserva; Inversiones a plazo fijo con las mejores tasas del mercado; las mismos que permiten a los socios de la Cooperativa, financiarlos créditos: Anticipo de Sueldo, Emergencia, Ordinario, y CrediFLASH, de acuerdo a su necesidad y capacidad de pago, con un monto máximo de 20.000 dólares.

La CACECH, premia la fidelidad de sus socios al entregar el aguinaldo navideño en Diciembre de cada año.

Para aquellos socios que han tenido la pérdida de su cónyuge, la CACECH, se solidariza en esos momentos difíciles con la entrega del seguro de vida familiar.

Y para aquellos socios que han depositado su confianza en nuestra Cooperativa, al realizar inversiones a plazo fijo; la CACECH, rifa un vehículo cero kilómetros anualmente.

Elaborado por: EGMA	**Fecha:** 2015-08-08
Revisado por: VSHB	**Fecha:** 2015-08-08

	INFORMACIÓN GENERAL	**DP 2/6**

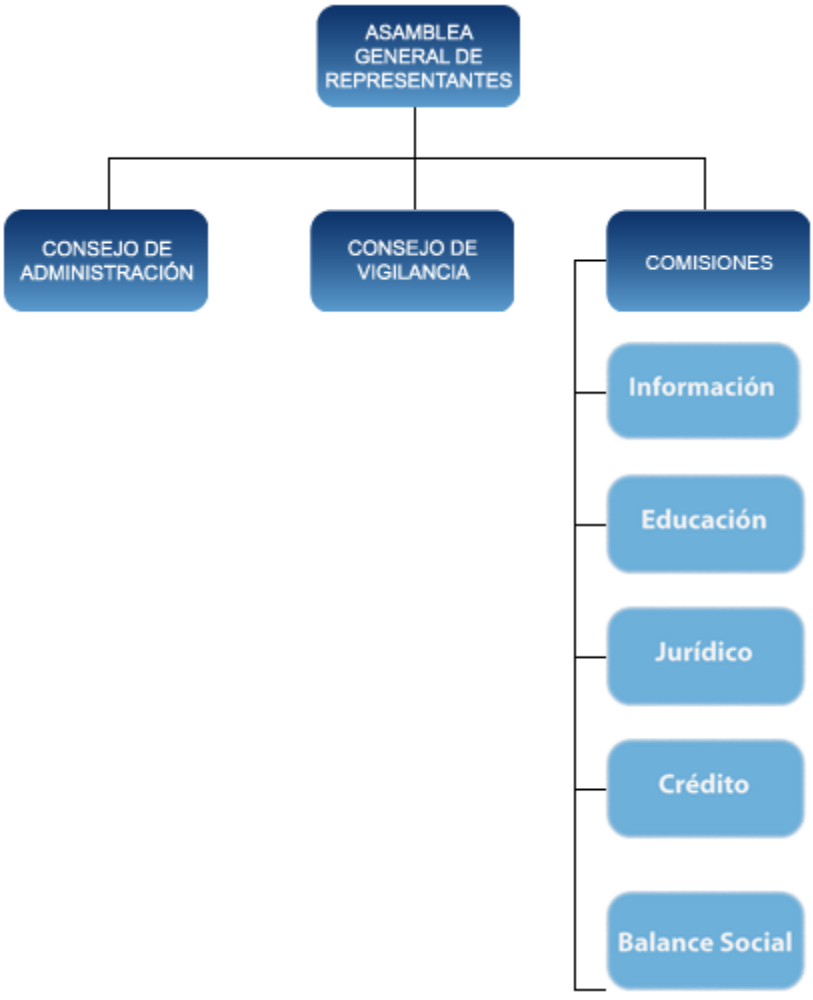
Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

La tarjeta de débito Visa Electrón CACECH, es el instrumento más solicitado por nuestros socios que se encuentran en los cantones más alejados de la provincia; pues, mediante ella pueden acceder al sueldo que mensualmente se deposita en su cuenta a través del Sistema de Pagos Interbancarios del Banco Central, en el menor tiempo del sector financiero.

La sinergia entre las políticas de sus Consejos de Administración, Vigilancia y Comisiones; las directrices de la Gerencia, el esfuerzo de su Talento Humano y sobre todo la confianza de sus Socios hacen que cada día sigamos creciendo y es por ello que la CACECH es "Cada día más ... GRANDE!! ".

Elaborado por: EGMA	**Fecha:** 2015-08-08
Revisado por: VSHB	**Fecha:** 2015-08-08

Gráfico 9: Gobierno Cooperativo de la CACECH

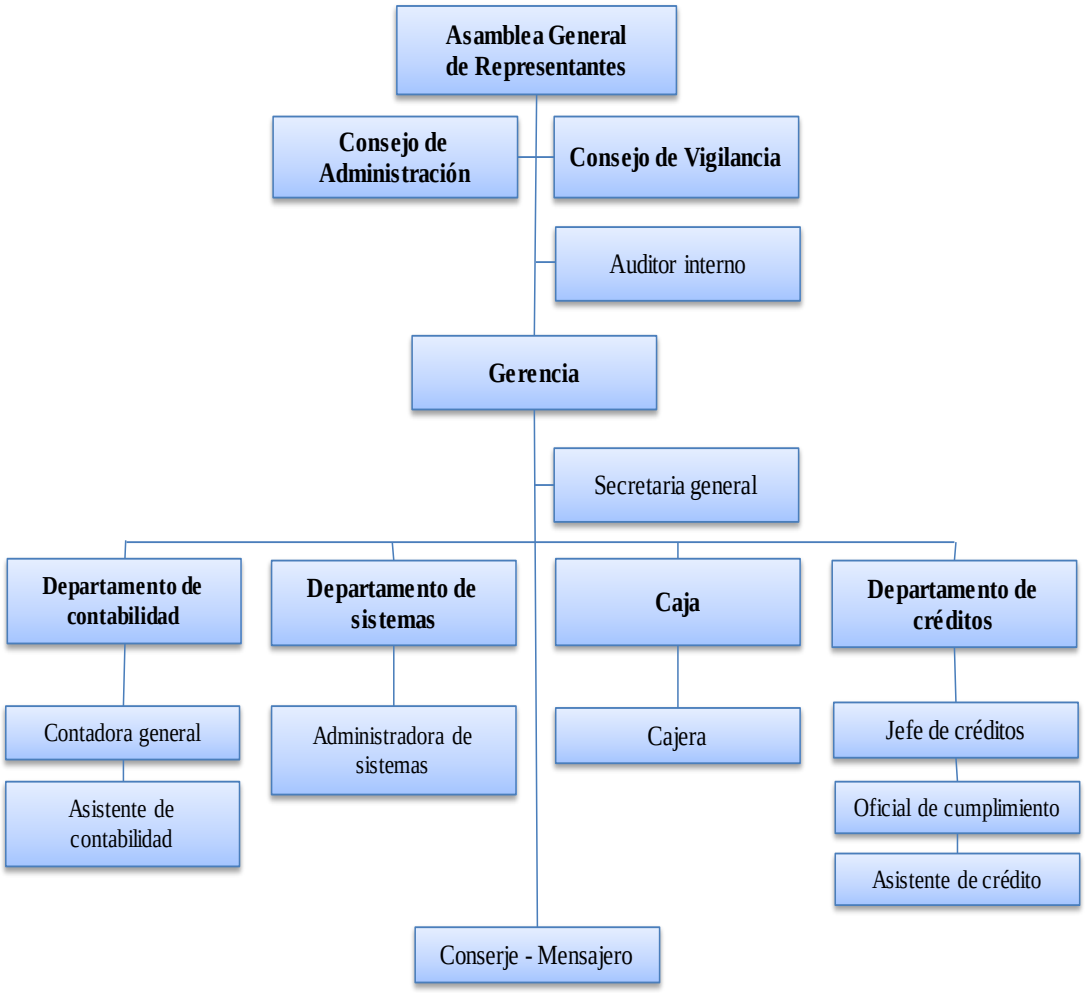


Fuente: Portala web CACECH (http://www.coaceducadoreschimborazo.fin.ec/index.php?option=com_content&view=article&id=13:gobierno-cooperativo&catid=4&Itemid=29)

	INFORMACIÓN GENERAL	**DP 4/6**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

Gráfico 10: Organigrama estructural



Fuente: Autor

* Éste organigrama ha sido elaborado (como sugerencia) en base a la información proporcionada en la página web de la CACECH.

Elaborado por: EGMA	**Fecha:** 2015-08-08
Revisado por: VSHB	**Fecha:** 2015-08-08

	INFORMACIÓN GENERAL	**DP 5/6**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

UBICACIÓN

País	Ecuador
Provincia	Chimborazo
Cantón	Riobamba
Dirección	José Veloz 22 – 11 y Eugenio Espejo (Esquina)

Gráfico 11: Ubicación CACECH

Fuente: Marble Virtual Globe

Elaborado por: EGMA	**Fecha:** 2015-08-08
Revisado por: VSHB	**Fecha:** 2015-08-08

	NORMATIVA	**DP 6/6**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

Se aplicará las siguientes normativas:

- Marco de referencia COBIT en su versión 4.1
- Normas ISO 27002

Cabe aclarar que las dos normas a ser usadas no son consideradas como normativa legal, más bien se les considera como un marco de referencia para la revisión de los sistemas informáticos.

Elaborado por: EGMA	**Fecha:** 2015-08-08
Revisado por: VSHB	**Fecha:** 2015-08-08

	PROPUESTA DE SERVICIOS PROFESIONALES	**PS 1/2**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

Riobamba, 10 de julio de 2015

Ingeniero

César Oña Mendoza

GERENTE GENERAL

Presente.-

De nuestra consideración:

Agradecemos la oportunidad de presentar nuestra propuesta de **AUDITORÍA DE SISTEMAS INFORMÁTICOS EN LA COOPERATIVA DE AHORRO Y CRÉDITO EDUCADORES DE CHIMBORAZO LTDA.**, **período 2014.**

Nuestra propuesta de servicios ha sido elaborada para dar respuesta a cada uno de sus requerimientos, tomando en cuenta el alcance de la Auditoría de Sistemas Informáticos, las Normas COBIT 4.1, NORMAS ISO 27002 y demás disposiciones legales que regulan las actividades de la Cooperativa.

Le manifestamos nuestro compromiso personal de entregarles un informe de auditoría eficiente y altamente coordinado de la manera más profesional y eficiente, construyendo una relación de confianza y de largo plazo mediante recomendaciones a ser implementadas. La naturaleza de nuestro trabajo es la ejecución de sistemas informáticos.

Elaborado por: EGMA	**Fecha:** 2015-08-10
Revisado por: VSHB	**Fecha:** 2015-08-10

	PROPUESTA DE SERVICIOS PROFESIONALES	**PS 2/2**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

Por lo cual la realización de la Auditoría de Sistemas Informáticos, se realizará de acuerdo con las prescripciones legales, normas internacionales, además se evaluará el control interno y el cumplimiento de las disposiciones legales y se determinará la falencias y sustentar con evidencias para elaborar el informe con las conclusiones y recomendaciones a ser utilizadas por la administración para una adecuada y correcta toma de decisiones, de la Cooperativa.

Contamos con equipo profesional con experiencia y desde ya, quedamos a su disposición.

Por la atención a la presente, nuestros más sinceros agradecimientos.

Atentamente

Michael Adrián Erazo Granizo
Auditor ME Auditores Independientes

Elaborado por: EGMA	**Fecha:** 2015-08-10
Revisado por: VSHB	**Fecha:** 2015-08-10

CC

CARTA DE COMPROMISO

No. 001

Riobamba, 13 de agosto de 2015

Señores.
AUDITORES

Presente.

De mi consideración:

Después de la visita preliminar que ha sido realizada a la **CACECH**, y posteriormente a la reunión llevada a cabo con el Gerente General, se ha resuelto autorizar la realización de la auditoría de sistemas informáticos a la institución, por el período 2014, para conocimiento y a fin de iniciar el correspondiente trabajo, cumplo en notificar que la oferta profesional ha sido aceptada, por lo que solicitamos absoluta confidencialidad con la información y responsabilidad en su labor; esperando que nuestro personal les dé la mejor atención en beneficio de la evaluación a realizarse y nos dé los mejores resultados en beneficio de la institución.

Atentamente,

Ing. CÉSAR OÑA MENDOZA, MBA
Gerente General CACECH

COOPERATIVA DE AHORRO Y CREDITO EDUCADORES DE CHIMBORAZO LTDA
CACECH
GERENCIA

OT

ORDEN DE TRABAJO

No.001

Riobamba, 13 de agosto de 2015

Señor

Michael Adrián Erazo Granizo

EGRESADO DE LA ESCUELA DE INGENIERÍA EN CONTABILIDAD Y AUDITORÍA

Presente:

En cumplimiento del Trabajo de titulación aprobado por el Consejo Directivo de la Facultad de Administración de Empresas, Escuela de Contabilidad y Auditoría, sírvase proceder a efectuar la **AUDITORÍA DE SISTEMAS INFORMÁTICOS EN LA COOPERATIVA DE AHORRO Y CRÉDITO EDUCADORES DE CHIMBORAZO LTDA.**, **período 2014.**

Se faculta al señor Michael Adrián Erazo Granizo que actué en calidad de auditor externo y el suscrito como supervisor. Terminando el Trabajo, se servirá presentar el respectivo informe.

Atentamente,

Ing. Hugo Bolívar Veloz Segovia
DIRECTOR

	CONTRATO POR PRESTACIÓN DE SERVICIOS DE AUDITORÍA	**CT 1/5**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

Comparecen a la celebración del presente contrato por una parte la Cooperativa de Ahorro y Crédito Educadores de Chimborazo Ltda., domiciliada en la ciudad de Riobamba, representada por el Ing. César Oña Mendoza a quien en adelante y para efectos del presente contrato se le denominara **CONTRATANTE**; y por parte ME Auditores Independientes, el auditor Michael Adrián Erazo Granizo con C.I.: 060411997-4, con domicilio principal en la ciudad de Riobamba debidamente autorizadas de sus propios derechos, quien en adelante se les denominará **CONTRATISTAS**; hemos celebrado el contrato de prestación de servicios profesionales de Auditoría de Sistemas Informáticos que se regirá por las siguientes cláusulas:

Primera – Objeto: Los contratistas de ME Auditores Independientes se obligan a cumplir la labor de auditoría de los sistemas informáticos de la Cooperativa de Ahorro y Crédito Educadores de Chimborazo Ltda., por el período económico 2014, de acuerdo por lo establecido en la Ley y en un todo de conformidad con la propuesta que presentó el Contratante en el mes de marzo del 2015, que para el efecto de descripción de funciones se considera incorporada al presente contrato.

Segunda – Duración: El presente contrato tendrá vigencia de tres (3) meses, comprendido desde el mes de julio y el mes de septiembre del 2014, entendiéndose el período sobre el cual se ejecutará el trabajo es el año calendario comprendido entre el 1 de Enero y el 31 de diciembre del mismo año. No obstante lo anterior, los contratistas de ME Auditores Independientes continuarán ejerciendo con las labores contratadas sin solución de continuidad hasta tanto no se notifique de la intención del CONTRATANTE de dar por terminado el contrato y en todo caso de conformidad con lo estipulado en la cláusula novena de este contrato.

Elaborado por: EGMA	**Fecha:** 2015-08-14
Revisado por: VSHB	**Fecha:** 2015-08-14

	CONTRATO POR PRESTACIÓN DE SERVICIOS DE AUDITORÍA	**CT 2/5**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

Tercera – Valor y Forma de Pago: El contratante no reconocerá a los contratistas independientes, como precio de este contrato y por la sola prestación de servicios descritos en la propuesta de que trata la Cláusula Primera de este documento, Por cuanto permitirá obtener el Título de Ingeniero en Contabilidad y Auditoría y un aporte a la Cooperativa de Ahorro y Crédito Educadores de Chimborazo Ltda.

Cuarto – Designaciones: Para el correcto cumplimiento de sus funciones, los contratistas de ME Auditores Independientes designarán a las personas que habrán de cumplir con las obligaciones que por este contrato asume, las cuales deben llenar los requisitos que para este tipo de funcionarios exige la ley, entre estas personas y el contratante no existirá ninguna relación de carácter laboral, y por ende, el pago de sus salarios y demás prestaciones sociales es responsabilidad exclusiva de los contratistas independientes.

Parágrafo: Además del citado personal, el contratante designará su nómina los funcionarios que se requieran para que presten su colaboración a la auditoría integral.

Quinta – Obligaciones del Contratante: Además de las obligaciones generales derivadas del presente contrato, el Contratante se compromete a a) Prestarle toda colaboración que soliciten los contratistas independientes facilitándoles todos los documentos o informes para que se requieran para el correcto cumplimiento de sus funciones; b) En caso de documentos que deban ser revisados y/o certificados por los contratistas independientes para su posterior presentación a entidades oficiales o particulares, El Contratante se obliga a entregar dichos documentos a los contratistas independientes con no menos de cinco (5) días hábiles de anticipación a la fecha de vencimiento de su presentación.

Elaborado por: EGMA	**Fecha:** 2015-08-14
Revisado por: VSHB	**Fecha:** 2015-08-14

Parágrafo: En caso de incumplimiento de cualesquiera de estas obligaciones por parte del contratante, en especial la contenida en el literal b) de ésta cláusula, los Contratistas de ME Auditores Independientes no serán responsables por demoras en la presentación de los documentos a las autoridades que lo requieran, pudiendo, además dejar constancia de las salvedades que consideren oportunas y quedando absolutamente libre de responsabilidad por errores u omisiones en que hayan incurrido el Contratante al diligenciar los documentos respectivos.

Sexta – Obligaciones de los Contratistas Independientes: Los Contratistas de ME Auditores Independientes se obligan únicamente y exclusivamente a la realización de las labores descritas en la propuesta presentada al Contratante y son los que corresponden a la auditoría de sistemas informáticos.

Séptima – Lugar de Presentación del Servicio: El servicio contratado por el contratante se prestará en la ciudad de Riobamba y se extenderá a otros lugares cuando por razón del servicio contratado se presentan circunstancias que lo requieran.

Octava – Domicilio Contractual: Para todos los efectos las partes acuerdan que sea en el domicilio contractual la ciudad de Riobamba.

	CONTRATO POR PRESTACIÓN DE SERVICIOS DE AUDITORÍA	**CT 4/5**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

Novena – Terminación del Contrato: Sin perjuicio de lo dispuesto en la cláusula segunda de este documento, el Contratante podrá dar por terminado este contrato en forma unilateral sujetándose a las siguientes previsiones: a) Antes del cumplimiento del plazo inicial de tres (3) meses pactado, en cualquier momento, pagando a los Contratistas de ME Auditores Independientes el precio total acordado en la cláusula tercera, el aviso de determinación del contrato debe ser dado a los contratistas independientes por lo menos con treinta (30) días calendario de anticipación a la fecha efectiva de dicha terminación.

Décima – Dotaciones y Recursos: El Contratante facilitará a su coste a los contratistas de ME Auditores Independientes el espacio físico, así como los elementos necesarios requeridos para el desempeño de su labor, tales como equipo de cálculo, mesas, sillas, etc.

Décima Primera – Autonomía de los Contratistas Independientes: En el desarrollo del presente contrato de prestación de servicios profesionales de auditoría de sistemas informáticos, los Contratistas de ME Auditores Independientes actúan como tal, realizando la labor encomendada con libertad y autonomía técnica y directiva.

Décima Segunda – Gastos: Los gastos en que se incurra como consecuencia de la celebración del presente contrato, como el pago del impuesto, publicaciones, etc., sea sufragados por partes iguales entre los contratantes.

Elaborado por: EGMA	**Fecha:** 2015-08-14
Revisado por: VSHB	**Fecha:** 2015-08-14

AUDITORES INDEPENDIENTES	**CONTRATO POR PRESTACIÓN DE SERVICIOS DE AUDITORÍA**	**CT 5/5**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

Otros: Las partes dejan constancia de que por razón de definición de los esquemas operativos, este contrato se firma a la fecha.

Para constancia se firma en la ciudad de Riobamba, a los 14 días del mes de julio del 2015.

El Contratante

Ing. CÉSAR OÑA MENDOZA, MBA
Gerente General CACECH

C.I. 060110356-7

Contratista ME Auditores Independientes

C.I. 060411997-4

Elaborado por: EGMA	**Fecha:** 2015-08-14
Revisado por: VSHB	**Fecha:** 2015-08-14

	NOTIFICACIÓN DE INICIO DE LA AUDITORÍA	**NI**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

Riobamba, 15 de agosto del 2015

Ingeniero
César Oña Mendoza
GERENTE GENERAL

Presente.-

De mi consideración:

De conformidad con lo dispuesto en la cláusula **Segunda** del contrato celebrado para la ejecución de la auditoría, notifico a usted, que la firma auditora ME Auditores Independientes, se encuentra realizando la Auditoría a los sistemas informáticos, por el período comprendido entre el 01 de enero al 31 de diciembre de 2014.

Por lo cual solicitamos que se nos facilite la información necesaria para la ejecución de la auditoria, así como la colaboración de todos los empleados de la institución.

Atentamente,

Michael Adrián Erazo Granizo
Auditor de ME Auditores Independientes

Elaborado por: EGMA	**Fecha:** 2015-08-15
Revisado por: VSHB	**Fecha:** 2015-08-15

4.2.2.1.4 Perspectivas consideradas para la evaluación

Para la presente auditoría se evaluarán las tecnologías de la información (TI) de acuerdo a los parámetros de revisión que plantea COBIT en su versión 4.1 quedando así:

- Planear y Organizar
- Adquirir e Implementar
- Entregar y Dar Soporte
- Monitorear y Evaluar

Sin embargo para mejor comprensión de los involucrados y facilidad en la ejecución se ha divido tanto para la elaboración de los programas específicos y los cuestionarios de la siguiente manera: seguridad física, seguridad lógica, TIC y gestión informática. Ésta división no perjudica a la anterior de ninguna manera, ya que su objetivo es solo recolectar información y se adaptará a la descrita en primer lugar para continuar con el trabajo sin ningún obstáculo.

4.2.2.1.5 Plan de auditoría

AUDITORES INDEPENDIENTES	**PLAN DE AUDITORÍA**	**PA 1/1**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

No.	Actividad	Responsable	Semanas							
			1	2	3	4	5	6	7	8
1	Elaborar plan de auditoría	Michael Erazo								
2	Aprobar plan de auditoría	Ing. Hítalo Veloz								
3	Preparar instrumentos	Michael Erazo								
4	Realizar visita preliminar	Michael Erazo								
5	Iniciar auditoría	Michael Erazo								
6	Auditar las TIC de la entidad	Michael Erazo								
10	Presentar borrador del informe	Michael Erazo								
11	Emitir informe final	Michael Erazo								
12	Comunicar resultados	Michael Erazo								

Elaborado por: EGMA	**Fecha:** 2015-09-03
Revisado por: VSHB	**Fecha:** 2015-09-03

4.2.2.1.6 Presupuesto

	PRESUPUESTO GENERAL	PG

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

No.	Artículo	Cantidad	Unidad	Costo	Total
1	Honorarios profesionales	-	-	-	0,00
2	Computador*	1	Unidades	600,00	600,00
3	Impresora*	1	Unidades	225,00	225,00
4	Celular*	1	Unidades	200,00	200,00
5	Calculadora*	1	Unidades	20,00	20,00
6	Unidad Flash USB*	1	Unidades	8,00	8,00
7	Cuaderno	1	Unidades	1,25	1,25
8	Hojas papel bond tamaño A4	2	Resmas	3,50	7,00
9	Lápiz 2B	4	Unidades	0,60	2,40
10	Esferos	6	Unidades	0,30	1,80
11	Borrador	2	Unidades	0,15	0,30
12	Resaltador	1	Unidades	0,75	0,75
13	Transporte	10	Veces	0,25	2,50
14	Protector de documentos	10	Unidades	0,15	1,50
15	Carpetas	2	Unidades	0,75	1,50
16	Papel adhesivo para notas	1	Paquetes	1,10	1,10
17	Impresiones	300	Unidades	0,01	3,00
	TOTAL				$ 1076,10

(*) Este artículo no ha sido adquirido exclusivamente para el desarrollo del presente trabajo ya que era parte de nuestro inventario con anterioridad, sin embargo, ha sido considerado dentro del presupuesto general debido al desgaste que sufre en el desarrollo del mismo.

Elaborado por: EGMA	**Fecha:** 2015-09-03
Revisado por: VSHB	**Fecha:** 2015-09-03

4.2.2.1.7 Programas específicos

	PROGRAMA DE AUDITORÍA SEGURIDAD LÓGICA	**PSL 1/4**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

	HECHO	POR	FECHA
I. Objetivos			
▪ Comprobar el software utilizado en la CACECH en su conjunto para determinar si cumple con todas las especificaciones técnicas, legales, sociales y por tanto si su uso proporciona resultados eficaces eficientes.			
II. Procedimientos			
1. Software del sistema (software de base) se deberá comprobar que:			
a) Existan control de modificaciones al sistema operativo.	✓	EGMA	Sept. 7
b) Que se evite realizar cambios no autorizados.	✓	EGMA	Sept. 7
c) Revisión de los procedimientos de obtención de backup.	✓	EGMA	Sept. 7
d) Existencia de la Metodología de selección de paquetes de software.	✓	EGMA	Sept. 7
e) Estado de las licencias.	✓	EGMA	Sept. 7
2. Efectúe revisión del Software de la base de datos y verifique que:			
a) La integridad de la base de datos.	✓	EGMA	Sept. 7
b) Que se hayan establecido estándares de documentación.	✓	EGMA	Sept. 7
c) Existencia de backup.	✓	EGMA	Sept. 7
d) Estado de las licencias.	✓	EGMA	Sept. 7

Elaborado por: EGMA	**Fecha:** 2015-09-03
Revisado por: VSHB	**Fecha:** 2015-09-03

	PROGRAMA DE AUDITORÍA SEGURIDAD LÓGICA	PSL 2/4

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

	HECHO	POR	FECHA
3. Revise el sistema de distribución y redes y compruebe:			
a) Provee abastecimiento de información.	✓	EGMA	Sept. 8
b) Existen planes de implantación y conversiones de la infraestructura de red.	✓	EGMA	Sept. 8
c) Existen estándares y políticas para el control de la red.	✓	EGMA	Sept. 8
d) Poseen facilidades de control del hardware y el software	✓	EGMA	Sept. 8
e) Existe compatibilidad y seguridad, en la integridad y el uso de datos.	✓	EGMA	Sept. 8
f) Existe control de acceso a datos en red.	✓	EGMA	Sept. 8
g) Existe un software de comunicación y sistema operativo de red – control de rendimiento de la red.	✓	EGMA	Sept. 8
4. Realice revisión de los sistemas locales y online para comprobar:			
a) Que el usuario tiene acceso directo al sistema y lo controla de algún modo a través de terminales del software disponible.	✓	EGMA	Sept. 8
b) Existen sistemas de consultas.	✓	EGMA	Sept. 8
c) Que se mantenga actualizado el software.	✓	EGMA	Sept. 8
d) Procedimientos de entrada de datos online (validaciones).	✓	EGMA	Sept. 8
e) Actualización de datos online.	✓	EGMA	Sept. 8

Elaborado por: EGMA	**Fecha:** 2015-09-03
Revisado por: VSHB	**Fecha:** 2015-09-03

	PROGRAMA DE AUDITORÍA SEGURIDAD LÓGICA	PSL 3/4

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

	HECHO	POR	FECHA
5. Indague y compruebe que ningún usuario puede acceder a datos que no debería o realizar procesos no permitidos, en este caso verifique:			
a) Que las passwords de los usuarios posean cambios periódicos.	✓	EGMA	Sept. 8
b) Perfiles de usuarios (acceso limitado a archivos).	✓	EGMA	Sept. 8
c) Bloqueo de terminales (time-out o intentos de acceso)	✓	EGMA	Sept. 8
d) Que las claves sean robustas.	✓	EGMA	Sept. 8
e) Exista control de acceso a los respaldos.	✓	EGMA	Sept. 8
f) Logueo de actividades del usuario.	✓	EGMA	Sept. 8
g) Encriptación de datos.	✓	EGMA	Sept. 8
6. Verifique los procedimientos de actualización online y compruebe:			
a) Automatización de las mismas.	✓	EGMA	Sept. 8
b) Existencia de Controles de acceso al sistema.	✓	EGMA	Sept. 8
c) Se establecen puntos de control en la entrada.	✓	EGMA	Sept. 8
d) Mantiene logs de actualizaciones.	✓	EGMA	Sept. 8
e) Se realizan validaciones sobre los registros actualizados.	✓	EGMA	Sept. 8
f) Proveen oportunamente la corrección de errores y su impacto.	✓	EGMA	Sept. 8
g) Mantienen una relación de los archivos que se hayan modificado, indicando el movimiento antes y después de la modificación.	✓	EGMA	Sept. 8

Elaborado por: EGMA	**Fecha:** 2015-09-03
Revisado por: VSHB	**Fecha:** 2015-09-03

	PROGRAMA DE AUDITORÍA SEGURIDAD LÓGICA	PSL 4/4

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

	HECHO	POR	FECHA
7. Realice análisis de la seguridad			
a) Disponibilidad de equipos alternativos para cubrir necesidades mínimas.	✓	EGMA	Sept. 8
b) Existencia de planes de emergencia, documentados y practicados.	✓	EGMA	Sept. 8
c) Seguridad de programas, archivos, backup, etc.	✓	EGMA	Sept. 8
d) Se utilizan protocoles de red seguros para transferencia de datos.	✓	EGMA	Sept. 8
e) Medidas de seguridad contra accesos no autorizados.	✓	EGMA	Sept. 8
8. Compruebe la aprobación de la implementación del software de sistemas nuevos y/o modificaciones al existente	✓	EGMA	Sept. 8

Elaborado por: EGMA	**Fecha:** 2015-09-03
Revisado por: VSHB	**Fecha:** 2015-09-03

	PROGRAMA DE AUDITORÍA SEGURIDAD FÍSICA	PSF 1/2

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

	HECHO	POR	FECHA
I. Objetivos			
▪ Comprobar la seguridad, calidad y uso eficiente de los equipos de escritorio, equipos servidores, infraestructura de red y de los periféricos complementarios que son propiedad de la entidad.			
▪ Verificar si existen medidas ante contingencias como incendio, inundaciones, huelgas, disturbios, sabotaje, etc. y continuar en medio de emergencia hasta que sea restaurado el servicio completo.			
II. Procedimientos			
1. Para el sistema central de la computadora y otras computadoras o servidores importantes soportados por este ambiente de procesamiento de la computadora, proporcione la siguiente información: a) Marca, modelo b) Sistema Operativo, versión c) Ubicación	✓	EGMA	Sept. 9
2. Investigar cómo se da mantenimiento al equipo de la computadora	✓	EGMA	Sept. 9
3. Asegurarse de que cualesquier cambio a los sistemas de aplicación se documenten adecuadamente.	✓	EGMA	Sept. 9
4. Que exista control y registro de las adquisiciones, cambios o disposiciones de hardware	✓	EGMA	Sept. 9

Elaborado por: EGMA	**Fecha:** 2015-09-03
Revisado por: VSHB	**Fecha:** 2015-09-03

	PROGRAMA DE AUDITORÍA SEGURIDAD LÓGICA	PSF 2/2

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

	HECHO	POR	FECHA
5. Compruebe que los ductos del aire están limpios, control de accesos restringido a los recursos, circuitos de vigilancia, registro de ingreso y egreso a recursos, respaldos en medios físicos, primordialmente.	✓	EGMA	Sept. 9
6. Verifique lo siguiente:			
a) En las instalaciones se debe tener equipo de fuente no interrumpible, tanto en la computadora como en la red y demás periféricos.	✓	EGMA	Sept. 9
b) Revisar el número de extintores, su capacidad, fácil acceso, y tipo de producto que utilizan.	✓	EGMA	Sept. 9
c) Investigar si el personal sabe usar los equipos contra incendio y si ha habido prácticas en cuanto a su uso.	✓	EGMA	Sept. 9
d) Se debe verificar que existan suficientes salidas de emergencia y que estén debidamente controladas para evitar robos por medio de estas salidas.	✓	EGMA	Sept. 9
e) Existan las seguridades suficientes como seguros, vigilancia, etc.	✓	EGMA	Sept. 9

Elaborado por: EGMA	**Fecha:** 2015-09-03
Revisado por: VSHB	**Fecha:** 2015-09-03

	PROGRAMA DE AUDITORÍA TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN	**PTC 1/4**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

	HECHO	POR	FECHA
I. Objetivos			
▪ Comprobar los medios de seguridad en la utilización de los equipos, accesos restringidos a programas, archivos y el monitoreo.			
▪ Verificar si el sistema de información proporciona información para planear, organizar y controlar de manera eficaz y oportuna para reducir la duplicidad de datos y de reportes y obtener una mayor seguridad en la forma más económica posible.			
II. Procedimientos			
1. Compruebe la existencia de medidas de seguridad siguientes:			
a) Se han restringido el acceso a sistemas operativos, a los programas y a los archivos.	✓	**EGMA**	Sept. 10
b) Los operadores trabajan con supervisión y no deben modificar los programas ni los archivos.	✓	**EGMA**	Sept. 10
c) Se aseguran en todo momento que los datos y archivos usados sean los adecuados, procurando no usar respaldos inadecuados.	✓	**EGMA**	Sept. 10
d) No se permite la entrada a la red a personas no autorizadas, ni a usar las terminales.	✓	**EGMA**	Sept. 10
e) Existe un registro de los accesos a la información sensible.	✓	**EGMA**	Sept. 10
f) Se realiza periódicamente una verificación física del uso de terminales y de los reportes obtenidos.	✓	**EGMA**	Sept. 10

Elaborado por: EGMA	**Fecha:** 2015-09-03
Revisado por: VSHB	**Fecha:** 2015-09-03

	PROGRAMA DE AUDITORÍA TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN	PTC 2/4

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

	HECHO	POR	FECHA
2. Verifique que los datos recolectados sean procesados completamente, por medio de los controles adecuados.			
a) Se controla la distribución de las salidas (reportes, informes, etc.).	✓	EGMA	Sept. 10
b) Se guardan copias de los archivos y programas en lugares ajenos al centro de cómputo y en las instalaciones de alta seguridad.	✓	EGMA	Sept. 10
c) Se tiene un estricto control sobre el acceso físico a los archivos.	✓	EGMA	Sept. 10
3. Compruebe la seguridad en el manejo de información:			
a) Que no se obtengan fotocopias de información confidencial sin la debida autorización.	✓	EGMA	Sept. 10
b) Sólo el personal autorizado debe tener acceso a la información confidencial.	✓	EGMA	Sept. 10
c) Control de los listados tanto de los procesos correctos como aquellos procesos con terminación incorrecta.	✓	EGMA	Sept. 10
d) Control del número de copias y la destrucción de la información y del papel carbón de los reportes muy confidenciales.	✓	EGMA	Sept. 10

Elaborado por: EGMA	**Fecha:** 2015-09-03
Revisado por: VSHB	**Fecha:** 2015-09-03

	PROGRAMA DE AUDITORÍA TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN	PTC 3/4

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

	HECHO	POR	FECHA
4. Verifique que la entidad cuente con los respaldos, y duplicados de los sistemas, programas, archivos y documentación necesarios.			
a) Equipo, programas y archivos	✓	EGMA	Sept. 11
b) Control de aplicaciones por terminal	✓	EGMA	Sept. 11
c) Definir una estrategia de seguridad de la red y de respaldos	✓	EGMA	Sept. 11
d) Requerimientos físicos.	✓	EGMA	Sept. 11
5. Compruebe si los sistemas son Integrados en un solo objetivo. Si existen sistemas que puedan ser interrelacionados y no programas aislados.	✓	EGMA	Sept. 11
6. Compruebe los niveles de seguridad si sólo las personas autorizadas tienen acceso y que no se duplique información.	✓	EGMA	Sept. 11
7. Compruebe si los sistemas son:			
a) Accesibles (que estén disponibles).	✓	EGMA	Sept. 11
b) Necesarios (que se pruebe su utilización).	✓	EGMA	Sept. 11
c) Comprensibles (que contengan todos los atributos).	✓	EGMA	Sept. 11
d) Oportunos (que esté la información en el momento que se requiere).	✓	EGMA	Sept. 11
e) Funcionales (que proporcionen la información adecuada a cada nivel).	✓	EGMA	Sept. 11
f) Estándar (que la información tenga la misma interpretación en los distintos niveles).	✓	EGMA	Sept. 11
g) Modernos			
h) Eficientes			
i) Herramientas para la toma de decisiones			

Elaborado por: EGMA	**Fecha:** 2015-09-03
Revisado por: VSHB	**Fecha:** 2015-09-03

	PROGRAMA DE AUDITORÍA TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN	PTC 4/4

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

	HECHO	POR	FECHA
8. Revise que:			
a) Se guardan copias periódicas de los archivos que permita reanudar un proceso a partir de una fecha determinada.	✓	EGMA	Sept. 11
b) Se puede reconfigurar los recursos disponibles, tanto de equipo y sistemas como de comunicaciones.	✓	EGMA	Sept. 11
9. Investigue si se contemplan procedimientos operativos de los recursos físicos como hardware y comunicaciones, planeando la utilización de equipos que permitan seguir operando en caso de falta de la corriente eléctrica, caminos alternos de comunicación y utilización de instalaciones de cómputo similares.	✓	EGMA	Sept. 11

Elaborado por: EGMA	**Fecha:** 2015-09-03
Revisado por: VSHB	**Fecha:** 2015-09-03

AUDITORES INDEPENDIENTES	**PROGRAMA DE AUDITORÍA GESTIÓN INFORMÁTICA**	**PGI 1/3**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

	HECHO	POR	FECHA
I. Objetivos			
▪ Comprobar si se gestiona de manera adecuada los recursos informáticos pertenecientes a la entidad y todo lo relacionado con las mismas.			
II. Procedimientos			
1. Compruebe si los responsables de la captura y modificación de la información están definidos, con claves de acceso de acuerdo a niveles.	✓	**EGMA**	Sept. 16
2. Verifique que no se tengan copias “piratas” o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus.	✓	**EGMA**	Sept. 16
3. Corrobore el uso inadecuado de la computadora			
a) la utilización de tiempo de máquina para usos ajenos de la organización.	✓	**EGMA**	Sept. 16
b) la copia de programas para fines de comercialización sin reportar los derechos de autor.	✓	**EGMA**	Sept. 16
c) el acceso a bases de datos a fin de modificar la información con propósitos fraudulentos.	✓	**EGMA**	Sept. 16
4. Compruebe que existan un método eficaz para proteger sistemas de computación es el software de control de acceso, tales como claves encriptadas de acceso.	✓	**EGMA**	Sept. 16

Elaborado por: EGMA	**Fecha:** 2015-09-03
Revisado por: VSHB	**Fecha:** 2015-09-03

	PROGRAMA DE AUDITORÍA GESTIÓN INFORMÁTICA	PGI 2/3

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

	HECHO	POR	FECHA
5. Identifique si el sistema integral de seguridad comprende:			
a) Elementos administrativos	✓	EGMA	Sept. 16
b) Definición de una política de seguridad	✓	EGMA	Sept. 16
c) Organización y división de responsabilidades	✓	EGMA	Sept. 16
d) Seguridad física y contra catástrofes (incendio, terremotos, etc.)	✓	EGMA	Sept. 16
e) Prácticas de seguridad del personal	✓	EGMA	Sept. 16
f) Elementos técnicos y procedimientos	✓	EGMA	Sept. 16
g) Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.	✓	EGMA	Sept. 16
h) Aplicación de los sistemas de seguridad, incluyendo datos y archivos	✓	EGMA	Sept. 16
6. Revise si se ha clasificado la instalación en términos de riesgo			
a) Se clasifican los datos, información y programas que contienen información confidencial que tenga un alto valor dentro del mercado de competencia de una organización, e información que sea de difícil recuperación.	✓	EGMA	Sept. 16
b) Se han identificado la información que tenga un gran costo financiero en caso de pérdida o bien puede provocar un gran impacto en la toma de decisiones.	✓	EGMA	Sept. 16

Elaborado por: EGMA	**Fecha:** 2015-09-03
Revisado por: VSHB	**Fecha:** 2015-09-03

	PROGRAMA DE AUDITORÍA **GESTIÓN INFORMÁTICA**	**PGI 3/3**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

	HECHO	POR	FECHA
7. Compruebe que se toman precauciones del riesgo que tenga la información con respecto al tipo y tamaño de la organización.			
a) El personal que prepara la información no debe tener acceso a la operación.	✓	**EGMA**	Sept. 16
b) Los operadores no debe tener acceso a las librerías ni a los lugares donde se tengan los archivos almacenados.	✓	**EGMA**	Sept. 16
c) Los operadores no deben ser los únicos que tengan el control sobre los trabajos procesados y no deben hacer las correcciones a los errores detectados.	✓	**EGMA**	Sept. 16

Elaborado por: EGMA	**Fecha:** 2015-09-03
Revisado por: VSHB	**Fecha:** 2015-09-03

4.2.2.1.8 Selección de métodos, técnicas, instrumentos y procedimientos

Cuadro 10: Selección de métodos, técnicas, instrumentos y procedimientos

Métodos	Técnicas	Instrumentos
Método investigación – acción Este tipo de investigación es adecuada ya que se requiere de conocimiento específico para éste problema en específico para ésta situación específica.	**Examen** Con el propósito de investigar algún hecho, comprobar alguna cosa, verificar la forma de realizar un proceso, evaluar la aplicación de las técnicas, métodos y procedimientos de trabajo, verificar el resultado de una transacción, comprobar la operación correcta de un sistema computacional.	**Cuestionario** El encuestado responderá de acuerdo con su criterio y personalmente; de esta manera se obtiene información útil que se puede concentrar, clasificar e interpretar por medio de su tabulación y análisis.
Método inductivo Se aplica para crear leyes a partir de la observación de los hechos, mediante la generalización del comportamiento observado.	**Inspección** Está relacionada con la aplicación de los exámenes que se realizarán para evaluar el funcionamiento de los sistemas; mediante la inspección se evaluará la eficiencia y eficacia del sistema.	**Entrevista** Para recopilar información en forma directa, cara a cara y a través de algún medio de captura de datos, es decir, el auditor interroga, investiga y confirma directamente con el entrevistado sobre los aspectos que está auditando.
Método hipotético-deductivo Se trata de establecer la verdad o falsedad de las hipótesis (que no podemos comprobar directamente, por su carácter de enunciados generales, o sea leyes, que incluyen términos teóricos), a partir	**Confirmación** Los resultados estarán fundamentados en información que sea plenamente comprobada y confirmada a través del uso de las técnicas, herramientas, procedimientos e instrumentos adecuados	**Encuesta** Es la recopilación de datos concretos sobre un tema específico, mediante el uso de cuestionarios o entrevistas diseñados con preguntas precisas para obtener las opiniones de los encuestados, las cuales permiten, después de hacer una rápida

de la verdad o falsedad de las consecuencias observacionales.	para la auditoría.	tabulación, análisis e interpretación.
	Comparación Con esto se obtendrá información relevante para la evaluación de la entidad evaluada, ya que se compara la forma en que debería funcionar y la forma en que está funcionando.	**Observación** Es el hecho de examinar, analizar, advertir o estudiar algo; se aplicará esta técnica para observar todo lo relacionado con los sistemas de una empresa.
	Revisión Documental Se revisan los manuales, instructivos, procedimientos diseñados para las funciones, actividades y operaciones, el registro de resultados, estadísticas y otros instrumentos de registro.	**Inventarios** Consiste en hacer un recuento físico de los equipos informáticos a fin de saber la cantidad existente en una fecha determinada y compararla con la que debería haber según los documentos en esa misma fecha.
	Matriz FODA o DOFA Con este documento se puede tener una apreciación preliminar sobre las fortalezas y debilidades del propio centro de información de la cooperativa, y se pueden analizar sus posibles amenazas y áreas de oportunidad.	**Experimentación** Como parte de la observación en la presente revisión, para poder ir adaptando o modificando sus variables conforme al plan programado, con el propósito de analizar sus posibles cambios.

Fuente: Resumen marco metodológico
Elaborado por: Autor

4.2.2.2 Ejecución de la auditoría

4.2.2.2.1 Cuestionario de control interno

AUDITORES INDEPENDIENTES	**CUESTIONARIO DE CONTROL INTERNO**	**CCI 1/4**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

PREGUNTAS	SI	NO	N/A	OBSERVS.
Control Interno General				
1. ¿Actualmente se cuenta con diagramas de las instalaciones de sistemas que posee la cooperativa?		x		
2. ¿Las funciones de control de inventarios, asignación de equipos, definición de funciones están separadas?	x			
3. ¿Tiene la cooperativa auditor interno? ¿De quién depende?	x			[3] Depende de los consejos de administración y vigilancia.
4. ¿Se tiene un catálogo de equipo, software y funciones del personal?	x			
5. ¿Actualmente existe algún manual o instructivo de asignación de equipo, de software, de mantenimiento, de operación?	x			[5] La encargada del área de sistemas tiene la buena costumbre de documentar la mayor cantidad posible de procesos.
6. ¿Se preparan y entregan a gerencia reportes periódicos de los activos tangibles o intangibles tecnológicos de la empresa?		x		[6] Existen reportes pero no se entregan.
7. ¿Se tiene control presupuestal de los costos y gastos?	x			
8. ¿Se hacen estudios y se documenta todo aquello que sirve para la determinación de una adquisición?	x			

Elaborado por: EGMA	**Fecha:** 2015-09-03
Revisado por: VSHB	**Fecha:** 2015-09-03

	CUESTIONARIO DE CONTROL INTERNO	CCI 2/4

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

PREGUNTAS	SI	NO	N/A	OBSERVS.
9. ¿Se ha definido una política general con respecto a contratación de seguros y monto de los mismos? ¿Revisa algún funcionario, el monto y la cobertura de los seguros?	x			
10. ¿Existe una revisión periódica de los mantenimientos preventivos? ¿En el área hay alguna persona encargada de supervisarlos y aprobarlos?	x			
11. ¿Se llevan a cabo revisiones periódicas de los sistemas para determinar si aún cumplen con los objetivos para los cuales fueron diseñados?	x			
12. ¿Tanto los datos como la información que procesa la entidad se almacena o se elimina de manera segura?	x			
13. ¿Existen medidas de contingencia en caso de flagelo o catástrofe?	x			
14. En el caso de servicios de terceros ¿Se tienen adecuadamente firmados los contratos explicando atribuciones u obligaciones de los mismos, así como sanciones/prestaciones en casos especiales?	x			

Elaborado por: EGMA	**Fecha:** 2015-09-03
Revisado por: VSHB	**Fecha:** 2015-09-03

	CUESTIONARIO DE CONTROL INTERNO	**CCI 3/4**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

PREGUNTAS	SI	NO	N/A	OBSERVS.
15. ¿Existen políticas implantadas para el descarte o desecho de los equipos que han alcanzado la máxima de su vida útil?	x			
16. ¿El acceso a la información es controlado completamente mediante el uso de claves u otros métodos?	x			
17. ¿Se aplican normas estandarizadas de alguna índole para el manejo de los equipos informáticos?				
18. ¿Se renuevan con regularidad los equipos a fin de mejorar los servicios prestados?	x			
19. ¿La redes (tanto intranet como internet) contemplan y dan servicio a todos los equipos de la cooperativa?	x			
20. ¿Se han realizado con anterioridad auditorías de sistemas informáticos o similares en la cooperativa?	x			
TOTAL	**17**	**3**	**0**	**Respuestas**
POSITIVAS	**85%**			
NEGATIVAS	**15%**			

Elaborado por: EGMA	**Fecha:** 2015-09-03
Revisado por: VSHB	**Fecha:** 2015-09-03

	CUESTIONARIO DE CONTROL INTERNO	**CCI 4/4**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

MEDICIÓN DE NIVELES DE RIESGO Y CONFIANZA

NIVEL DE CONFIANZA		
BAJO	**MEDIO**	**ALTO**
15 - 50	51 - 74	75 - 95
BAJO	**MEDIO**	**ALTO**
NIVEL DE RIESGO		

Análisis.- Para la aplicación del presente cuestionario de control interno se han tomado los aspectos más relevantes de cada revisión a realizarse para tener una base sólida sobre la cual desarrollar el trabajo.

Una vez terminada la aplicación del cuestionario de control interno se ha podido determinar que existe un ***nivel de confianza alto*** que corresponde al ***85%*** de respuestas afirmativas, esto garantiza que el examen a la institución puede realizarse por el auditor sin que el mismo comprometa o involucre al mismo en alguna forma; por otro lado existe un ***nivel de riesgo bajo*** correspondiente al ***15%*** de respuestas negativas lo que ayuda a confirmar que el trabajo puede proceder sin un gran riesgo aparente.

Elaborado por: EGMA	**Fecha:** 2015-09-03
Revisado por: VSHB	**Fecha:** 2015-09-03

4.2.2.2.2 Análisis FODA de los sistemas informáticos

Cuadro 11: Análisis FODA de la CACECH

FACTORES INTERNOS	FACTORES EXTERNOS
FORTALEZAS	**OPORTUNIDADES**
▪ Sistema institucional CONEXUS permite administración modular y centralizada de recursos, otorgando a cada usuario solo lo necesario para cumplir con sus actividades. ▪ El trabajo desplegado en el centro de cómputo está alineado con la misión y visión de la cooperativa. ▪ Mantenimiento preventivo y correctivo de los equipos. ▪ Software de acuerdo a las necesidades del negocio, actualizado constantemente. ▪ Software licenciado y actualizado. ▪ Equipos tecnológicos disponibles adecuados, suficientes y actualizados. ▪ Bitácoras con todas las incidencias, cambios y procedimientos. ▪ Documentación de soporte y procedimientos de casi la totalidad de procesos informáticos. ▪ Inventario completo y actualizado constantemente de los activos tecnológicos.	▪ Disponibilidad de encontrar en el mercado tecnologías de punta. ▪ Búsqueda de reducción de costos, aprovechando la aparición de nuevas tecnologías. ▪ Implementación y uso de software libre y gratuito equivalente al usado actualmente. ▪ Medidas adoptadas por los organismos de control como la Superintendencia de Economía Popular y Solidaria. ▪ Contratación de capacitación externa periódica. ▪ Incrementos en los salarios de los socios.

▪ Personal capacitado, experimentado y adecuado a los requerimientos en el departamento de sistemas. ▪ El personal administrativo ha recibido una adecuada inducción sobre el manejo de los equipos. ▪ Medidas contra ataques de software malicioso. ▪ Conexión en red en toda la cooperativa. ▪ Buen ambiente laboral.	✓ ✓	
DEBILIDADES		**AMENAZAS**
▪ Ambientes reducidos para los equipos. ▪ Infraestructura física poco adecuada. ▪ Funciones del personal de sistemas están definidas pero no se cumplen satisfactoriamente. ▪ Falta de recursos económicos para disponer una infraestructura informática más adecuada. ▪ Problemas con control de versiones de software. ▪ El personal no ha recibido por escrito las políticas de uso y mantenimiento de los equipos. ▪ Software de origen desconocido o innecesario.	✓ ☑ ✓ ☑	▪ Instituciones similares en el mercado. ▪ Elevados costos de hardware y software. ▪ Evolución constante de la tecnología. ▪ Fallos de los proveedores de bienes y servicios. ▪ Ingreso de agentes externos al departamento de sistemas sin ningún tipo de registro. ▪ Medidas adoptadas por los organismos de control como la Superintendencia de Economía Popular y Solidaria. ▪ Aparición constante de software malicioso. ▪ Cortes de energía eléctrica. ▪ Posibles sabotajes o intentos de intrusión a los sistemas por parte de personas ajenas a la cooperativa. ▪ Incremento de los gastos personales de los socios.

Fuente: Anexos 1 al 4
Elaborado por: Autor

a) Perfil estratégico interno CACECH

Cuadro 12: Perfil estratégico interno

	DEBILIDAD			FORTALEZA	
ASPECTOS INTERNOS	**Grave**	**Menor**	**Equidad**	**Normal**	**Relevante**
F1. Sistema institucional CONEXUS permite administración modular y centralizada de recursos, otorgando a cada usuario solo lo necesario para cumplir con sus actividades.					
F2. El trabajo desplegado en el centro de cómputo está alineado con la misión y visión de la cooperativa.					
F3. Mantenimiento preventivo y correctivo de los equipos.					
F4. Software de acuerdo a las necesidades del negocio, actualizado constantemente.					
F5. Software licenciado y actualizado.					
F6. Equipos tecnológicos disponibles adecuados, suficientes y actualizados.					
F7. Bitácoras con todas las incidencias, cambios y procedimientos.					
F8. Documentación de soporte y procedimientos de casi la totalidad de procesos informáticos.					
F9. Inventario completo y actualizado constantemente de los activos tecnológicos.					
F10. Personal capacitado, experimentado y adecuado a los requerimientos en el departamento de sistemas.					
F11. El personal administrativo ha recibido una adecuada inducción sobre el manejo de los equipos.					
F12. Medidas contra ataques de software malicioso.					

F13. Conexión en red en toda la cooperativa.					
F14. Buen ambiente laboral.					
D1. Ambientes reducidos para los equipos.					
D2. Infraestructura física poco adecuada.					
D3. Funciones del personal de sistemas están definidas pero no se cumplen satisfactoriamente.					
D4. Falta de recursos económicos para disponer una infraestructura informática más adecuada.					
D5. Problemas con control de versiones de software.					
D6. El personal no ha recibido por escrito las políticas de uso y mantenimiento de los equipos.					
D7. Software de origen desconocido o innecesario.					
TOTAL	**0**	**7**	**0**	**9**	**5**
PORCENTAJE	**0%**	**33,33%**	**0%**	**42,86%**	**23,81%**

FUENTE: Investigación
ELABORADO POR: Autor

Para la evaluación interna 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

2 = debilidad menor

3 = equidad

4 = fortaleza normal

5 = fortaleza relevante

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

Ponderación perfil interno

Cuadro 13: Ponderación perfil estratégico interno

ASPECTOS INTERNOS	Ponderación	Calificación	Resultado ponderado
F1. Sistema institucional CONEXUS permite administración modular y centralizada de recursos, otorgando a cada usuario solo lo necesario para cumplir con sus actividades.	0,048	5	0,24
F2. El trabajo desplegado en el centro de cómputo está alineado con la misión y visión de la cooperativa.	0,048	5	0,24
F3. Mantenimiento preventivo y correctivo de los equipos.	0,048	4	0,192
F4. Software de acuerdo a las necesidades del negocio, actualizado constantemente.	0,048	5	0,24
F5. Software licenciado y actualizado.	0,048	4	0,192
F6. Equipos tecnológicos disponibles adecuados, suficientes y actualizados.	0,048	4	0,192
F7. Bitácoras con todas las incidencias, cambios y procedimientos.	0,048	5	0,24
F8. Documentación de soporte y procedimientos de casi la totalidad de procesos informáticos.	0,048	4	0,192
F9. Inventario completo y actualizado constantemente de los activos tecnológicos.	0,048	4	0,192
F10. Personal capacitado, experimentado y adecuado a los requerimientos en el departamento de sistemas.	0,048	5	0,24
F11. El personal administrativo ha recibido una adecuada inducción sobre el manejo de los equipos.	0,048	4	0,192
F12. Medidas contra ataques de software malicioso.	0,048	4	0,192
F13. Conexión en red en toda la cooperativa.	0,048	4	0,192
F14. Buen ambiente laboral.	0,048	4	0,192
D1. Ambientes reducidos para los equipos.	0,048	2	0,096
D2. Infraestructura física poco adecuada.	0,048	2	0,096
D3. Funciones del personal de sistemas están definidas pero no se cumplen satisfactoriamente.	0,048	2	0,096
D4. Falta de recursos económicos para disponer una infraestructura informática más adecuada.	0,048	2	0,096
D5. Problemas con control de versiones de software.	0,048	2	0,096

D6. El personal no ha recibido por escrito las políticas de uso y mantenimiento de los equipos.	0,048	2	0,096
D7. Software de origen desconocido o innecesario.	0,048	2	0,096
TOTAL	**1**	**75**	**3,60**

FUENTE: Análisis FODA
ELABORADO POR: Autor

ANÁLISIS.-

Como resultado del análisis se obtiene una nota por encima del promedio que es **3,60** esto quiere decir que los sistemas informáticos instalados en la CACECH tienen más fortalezas que debilidades, éste es un indicador muy favorable de que el trabajo se está realizando con eficacia y eficiencia para bien de los usuarios internos y externos.

Entre las fortalezas más destacables se puede mencionar las ventajas que ofrece tener un sistema institucional que centralice todas las operaciones de las señoras y señores empleados y de permisos a los mismos de trabajar solo con lo estrictamente inherente a sus funciones. Así mismo el software que usa la cooperativa es en su gran mayoría el necesario para cumplir con los objetivos y fines planteados evitando así que los equipos se saturen con procesos no necesarios. También se debe destacar el uso de bitácoras donde se registran todo tipo de percances y transacciones que ocurren a diario en lo referente a los sistemas informáticos, las mismas que sirven para poder rastrear errores pasados y así evitar redundancias en el sistema, finalmente, se puede mencionar que todo lo anterior no sería posible si el departamento de sistemas de la cooperativa no contase con personal adecuado que geste estas operaciones y mantenga constantemente a punto los equipos.

En cuanto a las debilidades detectadas se puede destacar que el departamento de sistemas no posee un espacio físico acorde a las necesidades ya que el espacio es reducido (aunque suficiente) y con una infraestructura física poco adecuada ya que el edificio donde funcionan los mismos no cuenta con las debidas ventilaciones y espacios antes mencionados. Otro problema es el ingreso de los socios a las inmediaciones del departamento de sistemas, lo cual según lo expresado por la administradora del sitio no debería suceder, sin embargo por cuestión de falta de personal, de espacio no se puede evitar y es ella misma quién atiende a los socios en busca de solucionar los problemas que se suscitan. Otro problema que se detecta es la falta de ciertos equipos, software e

infraestructura que se consideran importantes para mejorar, sin embargo, por falta de presupuesto no se han podido implementar ya que su costo es muy alto y hay que considerar que la cooperativa solo puede permitirse comprar aquello que esté enmarcado en su presupuesto.

Se ha detectado también que el personal de la cooperativa no ha recibido por escrito los manuales de uso o mantención de los equipos informáticos y expresan no conocer normas de cuidado más que aquellas básicas que se efectúan por sentido común.

Finalmente, se ha detectado la instalación de software en los equipos que no tiene que ver con los fines de la cooperativa, aunque esto solo se encontró en un mínimo número de equipos (portátiles) se podría decir que no implican riesgo para las operaciones normales.

b) Perfil estratégico externo CACECH

Cuadro 14: Perfil estratégico externo

	AMENAZA			OPORTUNIDAD	
ASPECTOS EXTERNOS	**Grave**	**Menor**	**Equidad**	**Normal**	**Relevante**
O1. Disponibilidad de encontrar en el mercado tecnologías de punta.					
O2. Búsqueda de reducción de costos, aprovechando la aparición de nuevas tecnologías.					
O3. Implementación y uso de software libre y gratuito equivalente al usado actualmente.					
O4. Contratación de capacitación externa periódica.					
O5. Incrementos en los salarios de los socios.					
O6. y A1. Medidas adoptadas por los organismos de control como la Superintendencia de Economía Popular y Solidaria.					
A2. Instituciones similares en el mercado.					
A3. Elevados costos de hardware y software.					
A4. Evolución constante de la tecnología.					
A5. Fallos de los proveedores de bienes y servicios.					
A6. Ingreso de agentes externos al departamento de sistemas sin ningún tipo de registro.					
A7. Aparición constante de software malicioso.					
A8. Cortes de energía eléctrica.					
A9. Posibles sabotajes o intentos de intrusión a los sistemas por parte de personas ajenas a la cooperativa					
A10. Incremento de los gastos personales de los socios.					
TOTAL	**4**	**5**	**1**	**4**	**1**
PORCENTAJE	**26,67%**	**33,32%**	**6,67%**	**26,67%**	**6,67%**

FUENTE: Investigación
ELABORADO POR: Autor

El medio externo es todo lo que ocurre en el entorno de la organización y que influye directa o indirectamente en el cumplimiento de su misión. El medio externo no es estático y los cambios son cada vez más rápidos, continuos que precisan ser conocidos e interpretados adecuada y permanentemente.

La clasificación que se usara en los parámetros será:

1 = amenaza grave
2 = amenaza menor
3 = equidad
4 = oportunidad normal
5 = oportunidad relevante

Ponderación perfil externo

Cuadro 15: Ponderación perfil estratégico externo

ASPECTOS EXTERNOS	Ponderación	Calificación	Resultado ponderado
O1. Disponibilidad de encontrar en el mercado tecnologías de punta.	0,067	4	0,268
O2. Búsqueda de reducción de costos, aprovechando la aparición de nuevas tecnologías.	0,067	5	0,335
O3. Implementación y uso de software libre y gratuito equivalente al usado actualmente.	0,067	4	0,268
O4. Contratación de capacitación externa periódica.	0,067	4	0,268
O5. Incrementos en los salarios de los socios.	0,067	4	0,268
O6. y A1. Medidas adoptadas por los organismos de control como la Superintendencia de Economía Popular y Solidaria.	0,067	3	0,201
A2. Instituciones similares en el mercado.	0,067	2	0,134
A3. Elevados costos de hardware y software.	0,067	1	
A4. Evolución constante de la tecnología.	0,067	2	0,134
A5. Fallos de los proveedores de bienes y servicios.	0,067	1	0,067
A6. Ingreso de agentes externos al departamento de sistemas sin ningún tipo de registro.	0,067	2	0,134
A7. Aparición constante de software malicioso.	0,067	2	0,134
A8. Cortes de energía eléctrica.	0,067	1	0,067
A9. Posibles sabotajes o intentos de intrusión a	0,067	1	0,067

los sistemas por parte de personas ajenas a la cooperativa.			
A10. Incremento de los gastos personales de los socios.	0,067	2	0,134
TOTAL	**1**	**38**	**2,546**

FUENTE: Análisis FODA
ELABORADO POR: Autor

ANÁLISIS.-

El promedio obtenido es de **2,546** lo cual está justamente en el promedio de cálculo, esto quiere decir que la cooperativa CACECH tiene una relación neutra con el entorno externo, es decir, que lo que ocurre en el exterior no afecta ni beneficia a la institución.

Dentro de las oportunidades se puede destacar la búsqueda de reducción de costos, aprovechando la aparición de nuevas tecnologías; ya que como se percibió en el análisis interno, uno de los problemas fundamentales que presenta la cooperativa es la falta de ciertos equipos, software e infraestructura justamente por la falta de presupuesto y al aprovechar ésta oportunidad se podría mejorar la situación de la cooperativa y mejorar su gestión informática.

Algo que se puede destacar son las medidas adoptadas por los organismos de control, mismas que pueden ser consideradas tanto una oportunidad como una amenaza por el hecho de que a veces benefician o perjudican a las instituciones financieras o a sus socios, sumándoles o restándoles liquidez o capacidad de ahorro e inversión.

En cuanto a las amenazas, la mayoría de ellas son referentes a la adquisición de bienes y servicios, ya que muchas veces los mismos fallan de alguna manera causando interrupciones temporales del trabajo. Por suerte la cooperativa nunca ha sufrido ataques o intentos de intrusión a sus sistemas.

4.2.2.2.3 Revisión a los procesos aplicando COBIT 4.1

a) Matriz de riesgos y selección

Cuadro 16: Matriz de riesgos y selección

	Dominio principal analizado
	Subdominio analizado
	Dominio general no analizado

Importancia			Dominio	Proceso	Riesgo			Control de fuentes	
Alta	Media	Baja			Alto	Medio	Bajo	Documentado	No documentado
x			**PO1**	**Definir un Plan Estratégico de TI.**	x			x	
			PO1.1	Administración del Valor de TI		⊙			
			PO1.2	Alineación de TI con el Negocio	⊙				
			PO1.3	Evaluación del Desempeño y la Capacidad Actual		⊙			
			PO1.4	Plan Estratégico de TI		⊙			
			PO1.5	Planes Tácticos de TI		⊙			
			PO1.6	Administración del Portafolio de TI		⊙			
	x		**PO2**	**Definir la arquitectura de la Información.**	x			x	
			PO2.1	Modelo de Arquitectura de Información Empresarial		⊙			
			PO2.2	Diccionario de Datos Empresarial y Reglas de Sintaxis de Datos		⊙			
			PO2.3	Esquema de Clasificación de Datos	⊙				
			PO2.4	Administración de Integridad	⊙				
	x		**PO3**	**Determinar la Dirección Tecnológica.**			x	x	
			PO3.1	Planeación de la Dirección Tecnológica		⊙			
			PO3.2	Plan de Infraestructura Tecnológica		⊙			
			PO3.3	Monitoreo de Tendencias y Regulaciones Futuras		⊙			

			PO3.4	Estándares Tecnológicos		⊙			
			PO3.5	Consejo de Arquitectura de TI		⊙			
	x		**PO4**	**Definir los Procesos, Organización y Relaciones de TI.**			**x**	**x**	
			PO4.1	Marco de Trabajo de Procesos de TI		⊙			
			PO4.2	Comité Estratégico de TI		⊙			
			PO4.3	Comité Directivo de TI		⊙			
			PO4.4	Ubicación Organizacional de la Función de TI		⊙			
			PO4.5	Estructura Organizacional		⊙			
			PO4.6	Establecimiento de Roles y Responsabilidades		⊙			
			PO4.7	Responsabilidad de Aseguramiento de Calidad de TI		⊙			
			PO4.8	Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento		⊙			
			PO4.9	Propiedad de Datos y de Sistemas		⊙			
			PO4.10	Supervisión		⊙			
			PO4.11	Segregación de Funciones		⊙			
			PO4.12	Personal de TI		⊙			
			PO4.13	Personal Clave de TI		⊙			
			PO4.14	Políticas y Procedimientos para Personal Contratado		⊙			
			PO4.15	Relaciones		⊙			
x			**PO5**	**Administrar la Inversión en TI.**		**x**		**x**	
			PO5.1	Marco de Trabajo para la Administración Financiera		⊙			
			PO5.2	Prioridades Dentro del Presupuesto de TI		⊙			
			PO5.3	Proceso Presupuestal		⊙			
			PO5.4	Administración de Costos de TI		⊙			
			PO5.5	Administración de Beneficios		⊙			
x			**PO6**	**Comunicar las Aspiraciones y la Dirección de la Gerencia.**			**x**	**x**	
			PO6.1	Ambiente de Políticas y de Control		⊙			
			PO6.2	Riesgo Corporativo y Marco de Referencia de Control Interno de TI		⊙			
			PO6.3	Administración de Políticas para TI	⊙				
			PO6.4	Implantación de Políticas de TI	⊙				
			PO6.5	Comunicación de los Objetivos y la Dirección de TI		⊙			
x			**PO7**	**Administrar los Recursos Humanos de TI.**			**x**	**x**	
			PO7.1	Reclutamiento y Retención del Personal	⊙				

			PO7.2	Competencias del Personal	⊙				
			PO7.3	Asignación de Roles	⊙				
			PO7.4	Entrenamiento del Personal de TI		⊙			
			PO7.5	Dependencia Sobre los Individuos		⊙			
			PO7.6	Procedimientos de Investigación del Personal		⊙			
			PO7.7	Evaluación del Desempeño del Empleado		⊙			
			PO7.8	Cambios y Terminación de Trabajo		⊙			
	x		**PO8**	**Administrar la Calidad.**		**x**		**x**	
			PO8.1	Sistema de Administración de Calidad		⊙			
			PO8.2	Estándares y Prácticas de Calidad		⊙			
			PO8.3	Estándar es de Desarrollo y de Adquisición		⊙			
			PO8.4	Enfoque en el Cliente de TI		⊙			
			PO8.5	Mejora Continua		⊙			
			PO8.6	Medición, Monitoreo y Revisión de la Calidad		⊙			
	x		**PO9**	**Evaluar y Administrar los Riesgos de TI**		**x**		**x**	
			PO9.1	Marco de Trabajo de Administración de Riesgos	⊙				
			PO9.2	Establecimiento del Contexto del Riesgo		⊙			
			PO9.3	Identificación de Eventos		⊙			
			PO9.4	Evaluación de Riesgos de TI		⊙			
			PO9.5	Respuesta a los Riesgos		⊙			
			PO9.6	Mantenimiento y Monitoreo de un Plan de Acción de Riesgos		⊙			
	x		**PO10**	**Administrar Proyectos.**			**x**	**x**	
			PO10.1	Marco de Trabajo para la Administración de Programas		⊙			
			PO10.2	Marco de Trabajo para la Administración de Proyectos		⊙			
			PO10.3	Enfoque de Administración de Proyectos		⊙			
			PO10.4	Compromiso de los Interesados		⊙			
			PO10.5	Declaración de Alcance del Proyecto		⊙			
			PO10.6	Inicio de las Fases del Proyecto		⊙			
			PO10.7	Plan Integrado del Proyecto		⊙			
			PO10.8	Recursos del Proyecto		⊙			
			PO10.9	Administración de Riesgos del Proyecto		⊙			
			PO10.10	Plan de Calidad del Proyecto		⊙			
			PO10.11	Control de Cambios del Proyecto		⊙			
			PO10.12	Planeación del Proyecto y Métodos de Aseguramiento		⊙			

			PO10.13	Medición del Desempeño, Reporte y Monitoreo del Proyecto		⊙			
			PO10.14	Cierre del Proyecto		⊙			
	x		**AI1**	**Identificar Soluciones Automatizadas.**		**x**		**x**	
			AI1.1	Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio		⊙			
			AI1.2	Reporte de Análisis de Riesgos		⊙			
			AI1.3	Estudio de Factibilidad y Formulación de Cursos de Acción Alternativos		⊙			
			AI1.4	Requerimientos, Decisión de Factibilidad y Aprobación		⊙			
x			**AI2**	**Adquirir y Mantener Software Aplicativo.**		**x**		**x**	
			AI2.1	Diseño de Alto Nivel		⊙			
			AI2.2	Diseño Detallado		⊙			
			AI2.3	Control y Posibilidad de Auditar las Aplicaciones	⊙				
			AI2.4	Seguridad y Disponibilidad de las Aplicaciones	⊙				
			AI2.5	Configuración e Implantación de Software Aplicativo Adquirido	⊙				
			AI2.6	Actualizaciones Importantes en Sistemas Existentes		⊙			
			AI2.7	Desarrollo de Software Aplicativo		⊙			
			AI2.8	Aseguramiento de la Calidad del Software		⊙			
			AI2.9	Administración de los Requerimientos de Aplicaciones		⊙			
			AI2.10	Mantenimiento de Software Aplicativo		⊙			
x			**AI3**	**Adquirir y mantener infraestructura tecnológica.**		**x**		**x**	
			AI3.1	Plan de Adquisición de Infraestructura Tecnológica		⊙			
			AI3.2	Protección y Disponibilidad del Recurso de Infraestructura	⊙				
			AI3.3	Mantenimiento de la Infraestructura	⊙				
			AI3.4	Ambiente de Prueba de Factibilidad		⊙			
x			**AI4**	**Facilitar la Operación y el Uso.**		**x**		**x**	
			AI4.1	Plan para Soluciones de Operación		⊙			
			AI4.2	Transferencia de Conocimiento a la Gerencia del Negocio		⊙			
			AI4.3	Transferencia de Conocimiento a		⊙			

				Usuarios Finales					
			AI4.4	Transferencia de Conocimiento al Personal de Operaciones y Soporte		⊙			
	x		**AI5**	**Adquirir recursos de TI.**		**x**		**x**	
			AI5.1	Control de Adquisición	⊙				
			AI5.2	Administración de Contratos con Proveedores		⊙			
			AI5.3	Selección de Proveedores	⊙				
			AI5.4	Adquisición de Recursos de TI	⊙				
	x		**AI6**	**Administrar cambios.**			**x**	**x**	
			AI6.1	Estándares y Procedimientos para Cambios	⊙				
			AI6.2	Evaluación de Impacto, Priorización y Autorización		⊙			
			AI6.3	Cambios de Emergencia		⊙			
			AI6.4	Seguimiento y Reporte del Estatus de Cambio		⊙			
			AI6.5	Cierre y Documentación del Cambio	⊙				
	x		**AI7**	**Instalar y Acreditar Soluciones y Cambios.**		**x**		**x**	
			AI7.1	Entrenamiento		⊙			
			AI7.2	Plan de Prueba		⊙			
			AI7.3	Plan de Implantación		⊙			
			AI7.4	Ambiente de Prueba		⊙			
			AI7.5	Conversión de Sistemas y Datos		⊙			
			AI7.6	Pruebas de Cambios		⊙			
			AI7.7	Prueba de Aceptación Final		⊙			
			AI7.8	Promoción a Producción		⊙			
			AI7.9	Revisión Posterior a la Implantación		⊙			
x			**DS1**	**Definir y Administrar los Niveles de Servicio.**			**x**		**x**
			DS1.1	Marco de Trabajo de la Administración de los Niveles de Servicio		⊙			
			DS1.2	Definición de Servicios		⊙			
			DS1.3	Acuerdos de Niveles de Servicio		⊙			
			DS1.4	Acuerdos de Niveles de Operación		⊙			
			DS1.5	Monitoreo y Reporte del Cumplimento de los Niveles de Servicio	⊙				
			DS1.6	Revisión de los Acuerdos de Niveles de Servicio y de los Contratos		⊙			
	x		**DS2**	**Administrar los Servicios de Terceros.**		**x**		**x**	
			DS2.1	Identificación de Todas las Relaciones con Proveedores	⊙				

			DS2.2	Gestión de Relaciones con Proveedores		⭘			
			DS2.3	Administración de Riesgos del Proveedor	⭘				
			DS2.4	Monitoreo del Desempeño del Proveedor		⭘			
x			**DS3**	**Administrar el Desempeño y la Capacidad.**			**x**	**x**	
			DS3.1	Planeación del Desempeño y la Capacidad			⭘		
			DS3.2	Capacidad y Desempeño Actual			⭘		
			DS3.3	Capacidad y Desempeño Futuros			⭘		
			DS3.4	Disponibilidad de Recursos de TI			⭘		
			DS3.5	Monitoreo y Reporte					
x			**DS4**	**Garantizar la Continuidad del Servicio.**			**x**	**x**	
			DS4.1	Marco de Trabajo de Continuidad de TI			⭘		
			DS4.2	Planes de Continuidad de TI		⭘			
			DS4.3	Recursos Críticos de TI			⭘		
			DS4.4	Mantenimiento del Plan de Continuidad de TI			⭘		
			DS4.5	Pruebas del Plan de Continuidad de TI			⭘		
			DS4.6	Entrenamiento del Plan de Continuidad de TI			⭘		
			DS4.7	Distribución del Plan de Continuidad de TI			⭘		
			DS4.8	Recuperación y Reanudación de los Servicios de TI			⭘		
			DS4.9	Almacenamiento de Respaldos Fuera de las Instalaciones		⭘			
			DS4.10	Revisión Post Reanudación			⭘		
x			**DS5**	**Garantizar la Seguridad de los Sistemas.**		**x**		**x**	
			DS5.1	Administración de la Seguridad de TI		⭘			
			DS5.2	Plan de Seguridad de TI		⭘			
			DS5.3	Administración de Identidad		⭘			
			DS5.4	Administración de Cuentas del Usuario		⭘			
			DS5.5	Pruebas, Vigilancia y Monitoreo de la Seguridad	⭘				
			DS5.6	Definición de Incidente de Seguridad		⭘			
			DS5.7	Protección de la Tecnología de Seguridad		⭘			
			DS5.8	Administración de Llaves Criptográficas		⭘			
			DS5.9	Prevención, Detección y Corrección de Software Malicioso	⭘				
			DS5.10	Seguridad de la Red	⭘				
			DS5.11	Intercambio de Datos Sensitivos		⭘			

	x		**DS6**	**Identificar y Asignar Costos.**			**x**	**x**	
			DS6.1	Definición de Servicios			⭘		
			DS6.2	Contabilización de TI			⭘		
			DS6.3	Modelación de Costos y Cargos			⭘		
			DS6.4	Mantenimiento del Modelo de Costos			⭘		
	x		**DS7**	**Educar y Entrenar a los Usuarios.**			**x**	**x**	
			DS7.1	Identificación de Necesidades de Entrenamiento y Educación			⭘		
			DS7.2	Impartición de Entrenamiento y Educación			⭘		
			DS7.3	Evaluación del Entrenamiento Recibido			⭘		
	x		**DS8**	**Administrar la Mesa de Servicio y los Incidentes.**			**x**	**x**	
			DS8.1	Mesa de Servicios			⭘		
			DS8.2	Registro de Consultas de Clientes			⭘		
			DS8.3	Escalamiento de Incidentes			⭘		
			DS8.4	Cierre de Incidentes			⭘		
			DS8.5	Análisis de Tendencias			⭘		
	x		**DS9**	**Administrar la Configuración.**			**x**	**x**	
			DS9.1	Repositorio y Línea Base de Configuración			⭘		
			DS9.2	Identificación y Mantenimiento de Elementos de Configuración			⭘		
			DS9.3	Revisión de Integridad de la Configuración			⭘		
	x		**DS10**	**Administración de Problemas.**		**x**		**x**	
			DS10.1	Identificación y Clasificación de Problemas		⭘			
			DS10.2	Rastreo y Resolución de Problemas		⭘			
			DS10.3	Cierre de Problemas		⭘			
			DS10.4	Integración de las Administraciones de Cambios, Configuración y Problemas		⭘			
	x		**DS11**	**Administración de Datos.**		**x**		**x**	
			DS11.1	Requerimientos del Negocio para Administración de Datos		⭘			
			DS11.2	Acuerdos de Almacenamiento y Conservación	⭘				
			DS11.3	Sistema de Administración de Librerías de Medios		⭘			
			DS11.4	Eliminación		⭘			
			DS11.5	Respaldo y Restauración		⭘			
			DS11.6	Requerimientos de Seguridad para la Administración de Datos		⭘			

x			**DS12**	**Administración del Ambiente Físico.**		**x**		**x**	
			DS12.1	Selección y Diseño del Centro de Datos		⭘			
			DS12.2	Medidas de Seguridad Física	⭘				
			DS12.3	Acceso Físico	⭘				
			DS12.4	Protección Contra Factores Ambientales	⭘				
			DS12.5	Administración de Instalaciones Físicas		⭘			
	x		**DS13**	**Administración de Operaciones.**		**x**		**x**	
			DS13.1	Procedimientos e Instrucciones de Operación		⭘			
			DS13.2	Programación de Tareas		⭘			
			DS13.3	Monitoreo de la Infraestructura de TI		⭘			
			DS13.4	Documentos Sensitivos y Dispositivos de Salida		⭘			
			DS13.5	Mantenimiento Preventivo del Hardware		⭘			
	x		**ME1**	**Monitorear y Evaluar el Desempeño de TI.**		**x**		**x**	
			ME1.1	Enfoque del Monitoreo		⭘			
			ME1.2	Definición y Recolección de Datos de Monitoreo		⭘			
			ME1.3	Método de Monitoreo		⭘			
			ME1.4	Evaluación del Desempeño		⭘			
			ME1.5	Reportes al Consejo Directivo y a Ejecutivos		⭘			
			ME1.6	Acciones Correctivas		⭘			
x			**ME2**	**Monitorear y Evaluar el Control Interno.**		**x**		**x**	
			ME2.1	Monitoreo del Marco de Trabajo de Control Interno	⭘				
			ME2.2	Revisiones de Auditoría	⭘				
			ME2.3	Excepciones de Control		⭘			
			ME2.4	Control de Auto Evaluación		⭘			
			ME2.5	Aseguramiento del Control Interno	⭘				
			ME2.6	Control Interno para Terceros		⭘			
			ME2.7	Acciones Correctivas	⭘				
	x		**ME3**	**Garantizar el Cumplimiento con Requerimientos Externos.**		**x**			
			ME3.1	Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales		⭘			
			ME3.2	Optimizar la Respuesta a Requerimientos Externos		⭘			
			ME3.3	Evaluación del Cumplimiento con Requerimientos Externos		⭘			

			ME3.4	Aseguramiento Positivo del Cumplimiento		⊙			
			ME3.5	Reportes Integrados		⊙			
	x		**ME4**	**Proporcionar Gobierno de TI.**			**x**		
			ME4.1	Establecimiento de un Marco de Gobierno de TI			⊙		
			ME4.2	Alineamiento Estratégico			⊙		
			ME4.3	Entrega de Valor			⊙		
			ME4.4	Administración de Recursos			⊙		
			ME4.5	Administración de Riesgos			⊙		
			ME4.6	Medición del Desempeño			⊙		
			ME4.7	Aseguramiento Independiente			⊙		

FUENTE: COBIT 4.1, Anexo 1 - 2
ELABORADO POR: Autor

b) Criterios y recursos COBIT aplicables en la auditoría

Una vez terminada la matriz de riesgos y de selección mediante la aplicación de encuestas, entrevistas y criterios personales de la Administradora de sistemas de la cooperativa se ha considerado pertinente seleccionar determinados dominios y respectivos subdominios de COBIT aplicables para la auditoría en la cooperativa CACECH a fin de poder emitir criterios de juicio posteriormente.

En la siguiente tabla se ha realizado un compendio de los dominios de COBIT que fueron seleccionados, acompañados de los criterios de información que deben ser considerados para el análisis de cada uno de ellos y dándoles un nivel de importancia de P (Principal) y S (Secundario) a fin de saber qué criterio se debe tomar en cuenta y el orden en que se ha de realizar. También se han citado los recursos de TI dictaminados por COBIT para seleccionar cuáles de ellos participan en cada uno de los dominios.

Cuadro 17: Criterios aplicables en la auditoría

Dominio	Proceso	Criterios de información							Recursos de TI			
		Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	Aplicaciones	Información	Infraestructura	Personas
PLANEAR Y ORGANIZAR												
PO1	Definir un Plan Estratégico de TI	P	S						✓	✓	✓	✓
PO2	Definir la arquitectura de la Información.	S	P	S	P				✓	✓		
PO6	Comunicar las Aspiraciones y la Dirección de la Gerencia.	P					S			✓		✓
PO7	Administrar los Recursos Humanos de TI	P	P									✓
PO9	Evaluar y Administrar los Riesgos de TI	S	S	P	P	P	S	S	✓	✓	✓	✓
ADQUIRIR E IMPLEMENTAR												
AI2	Adquirir y Mantener Software Aplicativo	P	P		S			S	✓			
AI3	Adquirir y mantener infraestructura tecnológica	S	P		S	S					✓	
AI4	Facilitar la Operación y el Uso	P	P		S	S	S	S				
AI5	Adquirir recursos de TI	S	P				S		✓	✓	✓	✓
AI6	Administrar cambios	P	P		P	P		S	✓	✓	✓	✓
ENTREGAR Y DAR SOPORTE												
DS1	Definir y administrar los niveles de servicio	P	P	S	S	S	S	S	✓	✓	✓	✓
DS2	Administrar los servicios de terceros	P	P	S	S	S	S	S	✓	✓	✓	✓
DS3	Administrar el desempeño y la capacidad	P	P			S			✓		✓	
DS4	Garantizar la continuidad del servicio	P	S			P			✓	✓	✓	✓
DS5	Garantizar la seguridad de los sistemas			P	P	S	S	S	✓	✓	✓	✓
DS11	Administración de Datos.				P			P		✓		
DS12	Administración del ambiente físico				P	P					✓	

Dominio	Proceso	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	Aplicaciones	Información	Infraestructura	Personas
MONITOREAR Y EVALUAR												
ME2	Monitorear y evaluar el control interno	P	P	S	S	S	S	S	✓	✓	✓	✓
P = Primario S = Secundario												

FUENTE: Análisis FODA
ELABORADO POR: Autor

c) Análisis de subdominios

Los dominios y respectivos subdominios que resultaron seleccionados tras los análisis anteriores han de evaluarse a continuación, tratando de aportar la mayor cantidad de valor al estudio y a la vez procurando detectar posibles falencias del actual desarrollo de actividades relacionadas con las TI.

Se hará una relación con los enfoques del Gobierno de TI dictaminados para cada dominio, los cuales son:

- Alineación estratégica
- Entrega de valor
- Administración de Recursos
- Administración de Riesgos
- Medición del Desempeño

A los mismos se les dará un nivel de importancia a los mismos, entre P (Primario) y S (Secundario) para posteriormente poder construir una matriz que contenga las áreas focales beneficiadas con el examen.

PO1 Definir un plan estratégico.

Objetivo de control		Control a efectuar	Instrumentos aplicados	Documentación a revisar	Resultado
Subdominio	**Contenido**				
PO1.2 Alineación de TI con el Negocio	Educar a los ejecutivos sobre las capacidades tecnológicas actuales y sobre el rumbo futuro, sobre las oportunidades que ofrece TI, y sobre qué debe hacer el negocio para capitalizar esas oportunidades. Asegurarse de que el rumbo del negocio al cual está alineado TI está bien entendido. Las estrategias de negocio y de TI deben estar integradas, relacionando de manera clara las metas de la empresa y las metas de TI y reconociendo las oportunidades así como las limitaciones en la capacidad actual, y se deben comunicar de manera amplia. Identificar las áreas en que el negocio (estrategia) depende de forma crítica de TI, y mediar entre los imperativos del negocio y la tecnología, de tal modo que se puedan establecer prioridades concertadas.	Entrevista a la Administradora de sistemas. Revisión la existencia de un plan de capacitación sobre el uso de las TIC a los ejecutivos y/o administrativos. Revisión si éste plan estratégico de uso de las TIC está alineado con el plan del negocio.	Cuestionario Encuestas Entrevista Observación	Plan de capacitación de uso de las TIC. Plan estratégico cooperativa CACECH.	No existe un plan de capacitación sobre el uso de las TIC posterior al inicial, por tanto todo lo que conoce el personal administrativo y operacional sobre su uso y mantenimiento es producto de la inducción que reciben al iniciar sus actividades así como de su propia experiencia. Todas las áreas de la entidad dependen del uso de las TIC como prioridad para poder realizar sus operaciones. El uso de las TIC contribuye al cumplimiento de metas de la entidad en general.

Modelo de madurez

PO1 Definir un plan estratégico.

Administración del proceso de Definir un plan estratégico de TI que satisfaga el requerimiento de negocio de TI de sostener o extender la estrategia de negocio y los requerimientos de gobierno al mismo tiempo que se mantiene la transparencia sobre los beneficios, costos y riesgos es:

2 Repetible pero Intuitivo cuando

La planeación estratégica de TI se comparte con la gerencia del negocio según se necesite. La actualización de los planes de TI ocurre como respuesta a las solicitudes de la dirección. Las decisiones estratégicas se toman proyecto por proyecto, sin ser consistentes con una estrategia global de la organización. Los riesgos y beneficios al usuario, resultado de decisiones estratégicas importantes se reconocen de forma intuitiva.

P02. Definir la Arquitectura de la Información.

Objetivo de control		Control a efectuar	Instrumentos aplicados	Documentación a revisar	Resultado
Subdominio	**Contenido**				
PO2.3 Esquema de Clasificación de Datos	Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información (esto es, pública, confidencial, secreta) de la empresa. Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección, y una breve descripción de los requerimientos de retención y destrucción de datos, además de qué tan críticos y sensibles son. Se usa como base para aplicar controles como el control de acceso, archivo o cifrado.	Entrevista a la Administradora de sistemas. Revisión del esquema actual de clasificación de la información.	Cuestionario Encuestas Entrevista	Esquema de clasificación de la información.	Se aplica un esquema de clasificación de la información, el mismo se lo realiza de acuerdo al nivel de confidencialidad en: - Confidencial - Pública Y de acuerdo al nivel de relevancia en: - Vital - Esencial El mismo se halla documentado en la Secretaría de Consejo, además, los señores empleados conocen muy bien la clasificación de la información basados en su experiencia laboral. Cabe destacar que la CACECH no ha

					presentado problemas con el manejo de su información. Las herramientas de INFORMIX proveen la información referente a las bases de datos que se manejan.
PO2.4 Administración de Integridad	Definir e Implementar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y archivos.	Entrevista a la Administradora de sistemas. Revisión de documentos.	Cuestionario Encuestas Entrevista	Políticas del departamento de sistemas. Políticas generales.	Existen políticas para integridad de la información, mismas se aplican a la perfección en el departamento de sistemas y en el resto de la entidad.

Modelo de madurez

PO2 Definir la Arquitectura de la Información.

La administración del proceso de Definir la arquitectura de la información que satisface el requerimiento de negocio de TI de agilizar la respuesta a los requerimientos, para brindar información confiable y consistente y para integrar de forma transparente las aplicaciones hacia los procesos de negocio es:

3 Definido cuando

La importancia de la arquitectura de la información se entiende y se acepta, y la responsabilidad de su aplicación se asigna y se comunica de forma clara. Los procedimientos, herramientas y técnicas relacionados, aunque no son sofisticados, se han estandarizado y documentado y son parte de actividades informales de entrenamiento. Se han desarrollado políticas básicas de arquitectura de información, incluyendo algunos requerimientos estratégicos, aunque el cumplimiento de políticas, estándares y herramientas no se refuerza de manera consistente. Existe una función de administración de datos definida formalmente, que establece estándares para toda la organización, y empieza a reportar sobre la aplicación y uso de la arquitectura de la información.

Las herramientas automatizadas se empiezan a utilizar, aunque los procesos y reglas son definidos por los proveedores de software de bases de datos. Un plan formal de entrenamiento ha sido desarrollado, pero el entrenamiento formal se basa en iniciativas individuales.

PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia.

Objetivo de control		Control a efectuar	Instrumentos aplicados	Documentación a revisar	Resultado
Subdominio	**Contenido**				
PO6.3 Administración de Políticas para TI	Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI. Estas políticas deben incluir su intención, roles y responsabilidades, procesos de excepción, enfoque de cumplimiento y referencias a procedimientos, estándares y directrices. Su relevancia se debe confirmar y aprobar en forma regular.	Entrevista a la Administradora de sistemas. Revisión documental.	Cuestionario Encuestas Entrevista	Políticas del departamento de sistemas. Políticas generales.	Existen manuales de funciones establecidos, donde se detallan las funciones y atribuciones de los empleados, los mismos han sido desarrollados conforme a la política de seguridad de la entidad, pero no contemplan planes ni roles exclusivos para las TI. En el departamento de sistemas tiene documentación de la mayoría de procesos que allí se ejecutan.
PO6.4 Implantación de Políticas de TI	Asegurarse de que las políticas de TI se implantan y se comunican a todo el personal relevante, y se refuerzan, de tal forma que estén incluidas y sean parte integral de las operaciones empresariales.	Encuestas al personal de la entidad. Revisión documental. Bitácoras	Entrevista Observación		En el departamento de sistemas se conocen los procedimientos pertinentes para hacer frente a cualquier eventualidad.

Modelo de madurez

PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia.

La administración del proceso de Comunicar las aspiraciones y la dirección de la gerencia que satisfaga el requerimiento de negocio de TI de información precisa y oportuna sobre los servicios actuales de TI, riesgos asociados y responsabilidades es:

3 Definido cuando

La gerencia ha elaborado, documentado y comunicado un ambiente completo de administración de calidad y control de la información, que incluye un marco para las políticas, procedimientos y estándares. El proceso de elaboración de políticas es estructurado, mantenido y conocido por el personal, y las políticas, procedimientos y estándares existentes son razonablemente sólidos y cubren temas clave. La gerencia ha reconocido la importancia de la conciencia de la seguridad de TI y ha iniciado programas de concienciación. El entrenamiento formal está disponible para apoyar al ambiente de control de información, aunque no se aplica de forma rigurosa. Aunque existe un marco general de desarrollo para las políticas y estándares de control, el monitoreo del cumplimiento de estas políticas y estándares es inconsistente. Las técnicas para fomentar la conciencia de la seguridad están estandarizadas y formalizadas.

PO7 Administrar los Recursos Humanos de TI.

Objetivo de control		Control a efectuar	Instrumentos aplicados	Documentación a revisar	Resultado
Subdominio	**Contenido**				
PO7.1 Reclutamiento y Retención del Personal	Asegurarse que los procesos de reclutamiento del personal de TI estén de acuerdo a las políticas y procedimientos generales de personal de la organización (Ej. contratación, un ambiente positivo de trabajo y orientación). La gerencia implementa procesos para garantizar que la organización cuente con una fuerza de trabajo posicionada de forma apropiada, que tenga las habilidades necesarias para alcanzar las metas organizacionales.	Entrevistas a las señoras y señores empleados. Revisión documental.	Entrevista. Observación.	Políticas para la contratación de nuevo personal.	Existen políticas bien definidas en cuanto a la contratación del personal que maneja las TI de manera técnica en el departamento de sistemas y también para los administrativos; esto ha dado como consecuencia un buen manejo y conservación de los equipos, se puede ratificar indicando que no se han reportado problemas de fuerza mayor provocados por mal uso del personal.
PO7.2 Competencias del Personal	Verificar de forma periódica que el personal tenga las habilidades para cumplir sus roles con base en su educación, entrenamiento y/o experiencia. Definir los requerimientos esenciales de habilidades para TI y verificar que se les dé mantenimiento, usando	Revisión documental.	Entrevistas. Cuestionarios. Observación	Evaluaciones de desempeño. Métricas de desempeño requerido.	El personal actual posee las habilidades necesarias para operar de manera exitosa los equipos de la entidad. La administradora de sistemas posee el conocimiento y la experiencia necesaria para manejar y dar mantenimiento

	programas de calificación y certificación según sea el caso.				a los equipo de manera periódica.
PO7.3 Asignación de Roles	Definir, monitorear y supervisar los marcos de trabajo para los roles, responsabilidades y compensación del personal, incluyendo el requerimiento de adherirse a las políticas y procedimientos administrativos, así como al código de ética y prácticas profesionales. El nivel de supervisión debe estar de acuerdo con la sensibilidad del puesto y el grado de responsabilidades asignadas.		Entrevistas. Cuestionarios.		Marcos de trabajo para cada puesto bien definidos. No se han presentado problemas relacionados a la violación de políticas o falta de ética. El desempeño en cada puesto se supervisa de acuerdo al nivel de responsabilidad anexo al mismo.

Modelo de madurez

PO7 Administrar los Recursos Humanos de TI.

La administración del proceso de Administrar los recursos humanos de TI que satisfaga el requerimiento de negocio de TI de personal competente y motivado para crear y entregar servicios de TI es:

3 Definido cuando

Existe un proceso definido y documentado para administrar los recursos humanos de TI. Existe un plan de administración de recursos humanos. Existe un enfoque estratégico para la contratación y la administración del personal de TI. El plan de entrenamiento formal está diseñado para satisfacer las necesidades de los recursos humanos de TI. Está establecido un programa de rotación, diseñado para expandir las habilidades gerenciales y de negocio.

PO9 Evaluar y Administrar los Riesgos de TI.

Objetivo de control		Control a efectuar	Instrumentos aplicados	Documentación a revisar	Resultado
Subdominio	**Contenido**				
PO9.1 Marco de Trabajo de Administración de Riesgos	Establecer un marco de trabajo de administración de riesgos de TI que esté alineado al marco de trabajo de administración de riesgos de la organización.	Revisión del marco de trabajo de administración de riesgos de TI.	Entrevista. Revisión documental.	Marco de trabajo de administración de riesgos de TI.	No existe un marco de trabajo de administración de riesgos de TI. Los riesgos detectados se corrigen o se tratan conforme se detectan, procurando concordancia con los procedimientos generales de la cooperativa.

Modelo de madurez

PO9 Evaluar y Administrar los Riesgos de TI.

La administración del proceso de Evaluar y administrar los riesgos de TI que satisfaga el requerimiento de negocio de TI de analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y las metas de negocio es:

2 Repetible pero Intuitivo cuando

Existe un enfoque de evaluación de riesgos en desarrollo y se implementa a discreción de los gerentes de proyecto. La administración de riesgos se da por lo general a alto nivel y típicamente se aplica solo a proyectos grandes o como respuesta a problemas.

Los procesos de mitigación de riesgos están empezando a ser implementados donde se identifican riesgos.

AI2 Adquirir y Mantener Software Aplicativo

Objetivo de control		Control a efectuar	Instrumentos aplicados	Documentación a revisar	Resultado
Subdominio	**Contenido**				
AI2.3 Control y Posibilidad de Auditar las Aplicaciones	Implementar controles de negocio, cuando aplique, en controles de aplicación automatizados tal que el procesamiento sea exacto, completo, oportuno, autorizado y auditable.	Entrevista a la Administradora de sistemas.	Entrevista. Cuestionario.	Documentación referente al módulo de auditoría del sistema CONEXUS usado en la entidad. Bitácoras.	El sistema CONEXUS posee un módulo de auditoría que permite entregar un informe de las operaciones en cualquier momento. Al momento de la evaluación no se realizaba ya que el encargado del mismo recién asumía el cargo. El auditor interno no se acerca a solicitar reportes de auditoría.
AI2.4 Seguridad y Disponibilidad de las Aplicaciones	Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados y en línea con la clasificación de datos, la arquitectura de la información, la arquitectura de seguridad de la información y la tolerancia a riesgos de la organización.	Revisión documental.	Observación.	Bitácoras.	Las aplicaciones y el sistema en general están muy bien protegidas por software dedicado a dichas funciones. Además la disponibilidad de las aplicaciones fundamentales se da en base a las necesidades de cada trabajador.

AI2.5 Configuración e Implantación de Software Aplicativo Adquirido	Configurar e implementar software de aplicaciones adquiridas para conseguir los objetivos de negocio.	Revisión documental.	Observación. Entrevistas.	Manuales de software. Bitácoras.	Existen programas exclusivos dedicados a cumplir con los objetivos de la entidad.

Modelo de madurez

AI2 Adquirir y Mantener Software Aplicativo

La administración del proceso de Identificar soluciones automatizadas que satisfaga el requerimiento de negocio de TI de traducir los requerimientos funcionales y de control del negocio a diseño efectivo y eficiente de soluciones automatizadas es:

3 Definido cuando

Existen enfoques claros y estructurados para determinar las soluciones de TI. El enfoque para la determinación de las soluciones de TI requiere la consideración de alternativas evaluadas contra los requerimientos del negocio o del usuario, las oportunidades tecnológicas, la factibilidad económica, las evaluaciones de riesgo y otros factores. El proceso para determinar las soluciones de TI se aplica para algunos proyectos con base en factores tales como las decisiones tomadas por el personal involucrado, la cantidad de tiempo administrativo dedicado, y el tamaño y prioridad del requerimiento de negocio original. Se usan enfoques estructurados para definir requerimientos e identificar soluciones de TI.

AI3 Adquirir y Mantener Infraestructura Tecnológica

Objetivo de control		Control a efectuar	Instrumentos aplicados	Documentación a revisar	Resultado
Subdominio	**Contenido**				
AI3.2 Protección y Disponibilidad del Recurso de Infraestructura	Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad. Se deben definir y comprender claramente las responsabilidades al utilizar componentes de infraestructura sensitivos por todos aquellos que desarrollan e integran los componentes de infraestructura. Se debe monitorear y evaluar su uso.	Entrevista a la Administradora de sistemas. Revisión documental.	Cuestionarios. Entrevistas.	Medidas de control interno relacionadas a la protección de equipos y software.	Las medidas de protección de los equipo existen y están actualizadas. Comprenden todos los sistemas usados por la entidad.
AI3.3 Mantenimiento de la Infraestructura	Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.	Entrevista a la Administradora de sistemas.	Entrevistas.	Medidas de control interno relacionadas a la protección de equipos y software.	Ya existe un plan implantado de mantenimiento de la infraestructura, mismo que se actualiza y cambia conforme a la evolución y necesidades de la entidad.

Modelo de madurez

AI3 Adquirir y Mantener Infraestructura Tecnológica

La administración del proceso de Adquirir y mantener infraestructura de tecnología que satisfaga el requerimiento de negocio de TI de adquirir y mantener una infraestructura de TI integrada y estandarizada es:

4 Administrado y Medible cuando

Se desarrolla el proceso de adquisición y mantenimiento de la infraestructura de tecnología a tal punto que funciona bien para la mayoría de las situaciones, se le da un seguimiento consistente y un enfoque hacia la reutilización. La infraestructura de TI soporta adecuadamente las aplicaciones del negocio. El proceso está bien organizado y es preventivo. Tanto el costo como el tiempo de realización para alcanzar el nivel esperado de escalamiento, flexibilidad e integración se han optimizado parcialmente.

AI4 Facilitar la Operación y el Uso

Objetivo de control		Control a efectuar	Instrumentos aplicados	Documentación a revisar	Resultado
Subdominio	**Contenido**				
AI4.2 Transferencia de Conocimiento a la Gerencia del Negocio	Transferir el conocimiento a la gerencia de la empresa para permitirles tomar posesión del sistema y los datos y ejercer la responsabilidad por la entrega y calidad del servicio, del control interno, y de los procesos administrativos de la aplicación. La transferencia de conocimiento incluye la aprobación de acceso, administración de privilegios, segregación de tareas, controles automatizados del negocio, respaldo/recuperación, seguridad física y archivo de la documentación fuente.	Revisión documental. Entrevista a la Administradora de sistemas.	Entrevista. Cuestionarios Observación.	Documentación y políticas desarrolladas de manera interna en el departamento de sistemas. Manuales de productos.	Se ha documentado la gran mayoría de procesos dentro del área de sistemas y se ha transferido la información a la gerencia en caso de cambios de personal u otra situación.
AI4.3 Transferencia de Conocimiento a Usuarios Finales	Transferencia de conocimiento y habilidades para permitir que los usuarios finales utilicen con efectividad y eficiencia el sistema de aplicación como apoyo a los procesos del negocio. La transferencia de conocimiento incluye el desarrollo de un plan de entrenamiento que aborde al entrenamiento inicial y al continuo, así como el desarrollo de habilidades, materiales de entrenamiento, manuales de usuario, manuales de procedimiento, ayuda en línea, asistencia a usuarios, identificación del usuario clave, y evaluación.	Revisión documental.	Cuestionarios Observación.	Bitácoras Encuestas al personal	Todos los usuarios reciben inducción al iniciar sus funciones. Reciben documentación y soporte contínuo por parte de la administradora cada vez que hay cambios.

Modelos de madurez

AI4 Facilitar la Operación y el Uso

La administración del proceso de Facilitar la operación y el uso que satisfaga el requerimiento de negocio de TI de garantizar la satisfacción de los usuarios finales con ofrecimiento de servicios y niveles de servicio, e integrar de forma transparente aplicaciones y soluciones de tecnología dentro de los procesos del negocio es:

3 Definido cuando

Existe un esquema bien definido, aceptado y comprendido para documentación del usuario, manuales de operación y materiales de entrenamiento. Se guardan y se mantienen los procedimientos en una biblioteca formal y cualquiera que necesite saber tiene acceso a ella. La s correcciones a la documentación y a los procedimientos se realizan por reacción. Los procedimientos se encuentran disponible s fuera de línea y se pueden acceder y mantener en caso de desastre. Existe un proceso que especifica las actualizaciones de procedimientos y los materiales de entrenamiento para que sea un entregable explícito de un proyecto de cambio. A pesar de la existencia de enfoques definidos, el contenido actual varía debido a que no hay un control para reforzar el cumplimiento de estándares. Los usuarios se involucran en los procesos informalmente. Cada vez se utilizan más herramientas automatizadas en la generación y distribución de procedimientos. Se planea y programa tanto el entrenamiento del negocio como de los usuario.

AI5 Adquirir Recursos de TI

Objetivo de control		Control a efectuar	Instrumentos aplicados	Documentación a revisar	Resultado
Subdominio	**Contenido**				
AI5.1 Control de Adquisición	Desarrollar y seguir un conjunto de procedimientos y estándares consistente con el proceso general de adquisición es de la organización y con la estrategia de adquisición para adquirir infraestructura relacionada con TI, instalaciones, hardware, software y servicios necesarios por el negocio.	Revisión documental.	Observación. Entrevista.	Listado de proveedores. Contratos con proveedores. Facturas.	Existen procedimientos de adquisición bien implantados y conforme a las necesidades de la entidad para la compra de nuevos equipos.
AI5.3 Selección de Proveedores	Seleccionar proveedores de acuerdo a una práctica justa y formal para garantizar la mejor viable y encajable según los requerimientos especificados. Los requerimientos deben estar optimizados con las entradas de los proveedores potenciales.	Revisión documental.	Entrevista.	Listado de proveedores. Contratos con proveedores.	Por regla general se adquiere en su mayoría equipos marca HP por la garantía y soporte que brindan los proveedores. Los proveedores del servicio de internet son: Telconet y Puntonet. La instalación y mantenimiento de los servidores está a cargo de AVMEI Cía. Ltda., así

					como también el sistema financiero para Cooperativas de Ahorro y Crédito CONEXUS MILLENNIUM. El sistema institucional Informix e Informix REPLIX es proporcionado por IBM®. Los demás proveedores son seleccionados de acuerdo a compras anteriores y precios del mercado.
AI5.4 Adquisición de Recursos de TI	Proteger y hacer cumplir los intereses de la organización en todo los contratos de adquisiciones, incluyendo los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de software, recursos de desarrollo, infraestructura y servicios.	Revisión documental. Entrevista a la Administradora de Sistemas.	Observación. Entrevista	Contratos con proveedores.	Se ha detectado que el proveedor AVMEI Cía. Ltda. no cumple a satisfacción sus contratos, ya que no cumple a satisfacción con la cláusula de mantenimiento de los servidores que ha instalado.

Modelos de madurez

AI5 Adquirir Recursos de TI

La administración del proceso de Adquirir recursos de TI que satisfaga el requerimiento de negocio de TI de mejorar la rentabilidad de TI y su contribución a la utilidad del negocio es:

3 Definido cuando

La administración establece políticas y procedimientos para la adquisición de TI. Las políticas y procedimientos toman como guía el proceso general de adquisición de la organización. La adquisición de TI se integra en gran parte con los sistemas generales de adquisición del negocio. Existen estándares de TI para la adquisición de recursos de TI. Los proveedores de recursos de TI se integran dentro de los mecanismos de administración de proyectos de la organización desde una perspectiva de administración de contra tos.

La administración de TI comunica la necesidad de contar con una administración adecuada de adquisiciones y contratos en toda la función de TI.

AI6 Administrar cambios

Objetivo de control		Control a efectuar	Instrumentos aplicados	Documentación a revisar	Resultado
Subdominio	**Contenido**				
AI6.1 Estándares y Procedimientos para Cambios	Establecer procedimientos de administración de cambio formales para manejar de manera estándar todas las solicitudes (incluyendo mantenimiento y parches) para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio, y las plataformas fundamentales.	Revisión documental.	Entrevista. Observación.	Bitácoras.	Los procedimientos están estandarizados, tanto por los manuales de usuario entregados por los proveedores como por aquellos procesos exclusivos de la entidad que han sido documentados en las bitácoras y se han pasado a los manuales de procedimientos.
AI6.5 Cierre y Documentación del Cambio	Siempre que se implantan cambios al sistema, actualizar el sistema asociado y la documentación de usuario y procedimientos correspondientes. Establecer un proceso de revisión para garantizar la implantación completa de los cambios.	Revisión documental.	Entrevista. Observación.	Bitácoras.	Existe un buen nivel de control de los cambios de procesos y de sistema, éstos se documentan en las bitácoras con sus respectivos detalles, se actualizan sistemas y documentación.

Modelo de madurez

AI6 Administrar cambios

La administración del proceso de Administrar cambios que satisfaga el requerimiento de negocio de TI de responder a los requerimientos de acuerdo con la estrategia del negocio, mientras que se reducen los defectos y repeticiones de trabajos en la entrega de soluciones y servicios es:

5 Optimizado cuando

El proceso de administración de cambios se revisa con regularidad y se actualiza para permanecer en línea con las buenas prácticas.

El proceso de revisión refleja los resultados del monitoreo. La información de la con figuración es computarizada y proporciona un control de versión. El rastreo del cambio es sofisticado e incluye herramientas para detectar software no autorizado y sin licencia. La administración de cambio de TI se integra con la administración de cambio del negocio para garantizar que TI sea un factor que hace posible el incremento de productividad y la creación de nuevas oportunidades de negocio para la organización.

DS1 Definir y Administrar los Niveles de Servicio

Objetivo de control		Control a efectuar	Instrumentos aplicados	Documentación a revisar	Resultado
Subdominio	**Contenido**				
DS1.5 Monitoreo y Reporte del Cumplimento de los Niveles de Servicio	Monitorear continuamente los criterios de desempeño especificados para el nivel de servicio. Los reportes sobre el cumplimiento de los niveles de servicio deben emitirse en un formato que sea entendible para los interesados. Las estadísticas de monitoreo son analizadas para identificar tendencias positivas y negativas tanto de servicios individuales como de los servicios en conjunto.	Entrevista a la Administradora de sistemas. Revisión documental.	Observación.	Bitácoras.	Se lleva un registro de las incidencias reportadas por los señores socios de la cooperativa, mismo en el que se registran los problemas a fin de mejorar los servicios para los socios y llevar un histórico que permita solucionar futuros inconvenientes. No se han presentado incidencias de alto nivel.

Modelo de madurez

DS1 Definir y Administrar los Niveles de Servicio

La administración del proceso de Definir y administrar niveles de servicio que satisfacen el requerimiento de negocio para TI de asegurar la alineación de servicios claves de TI con la estrategia de negocio es:

3 Definido cuando

Las responsabilidades están bien definidas pero con autoridad discrecional. El proceso de desarrollo del acuerdo de niveles de servicio está en orden y cuenta con puntos de control para revalorar los niveles de servicio y la satisfacción de cliente. Los servicios y los niveles de servicio están definidos, documentados y se ha acordado utilizar un proceso estándar. Las deficiencias en los niveles de servicio están identificadas pero los procedimientos para resolver las deficiencias son informales. Hay un claro vínculo entre el cumplimiento del nivel de servicio esperado y el presupuesto contemplado. Los niveles de servicio están acordados pero pueden no responder a las necesidades del negocio.

DS2 Administrar los Servicios de Terceros

Objetivo de control		Control a efectuar	Instrumentos aplicados	Documentación a revisar	Resultado
Subdominio	**Contenido**				
DS2.1 Identificación de Todas las Relaciones con Proveedores	Identificar todos los servicios de los proveedores, y categorizarlos de acuerdo al tipo de proveedor, significado y criticidad. Mantener documentación formal de relaciones técnicas y organizacionales que cubren los roles y responsabilidades, metas, entregables esperados, y credenciales de los representantes de estos proveedores.	Entrevista a la Administradora de sistemas. Revisión documental.	Observación. Entrevista.	Listado de proveedores. Contratos con proveedores.	Existe documentación formal y completa de los proveedores que han realizado transacciones con la cooperativa como facturas, contratos, proformas, etc.
DS2.3 Administración de Riesgos del Proveedor	Identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener un efectivo servicio de entrega de forma segura y eficiente sobre una base de continuidad. Asegurar que los contratos están de acuerdo con los requerimientos legales y regulatorios de los estándares universales del negocio. La administración del riesgo debe considerar además acuerdos de confidencialidad (NDAs), contratos de garantía, viabilidad de la continuidad del proveedor, conformidad con los requerimientos de seguridad, proveedores alternativos, penalizaciones e incentivos, etc.	Entrevista a la Administradora de sistemas. Revisión documental.	Observación. Entrevista.	Contratos con proveedores.	Los contratos están bien formulados de acuerdo a las leyes y normativas vigentes en el Ecuador y especifican garantías, viabilidad de la continuidad del proveedor, conformidad con los requerimientos de seguridad, penalizaciones e incentivos. Todo esto considerando la calidad del servicio y de la información.

Modelo de madurez

DS2 Administrar los Servicios de Terceros

La administración del proceso de Administrar los servicios de terceros que satisfagan los requerimientos de TI del negocio de brindar servicios de terceros satisfactorios siendo transparentes respecto a los beneficios, costos y riesgos es:

3 Definido cuando

Hay procedimientos bien documentados para controlar los servicios de terceros con procesos claros para tratar y negociar con los proveedores. Cuando se hace un acuerdo de prestación de servicios, la relación con el tercero es meramente contractual. La naturaleza de los servicios a prestar se detalla en el contrato e incluye requerimientos legales, operativos y de control. Se asigna la responsabilidad de supervisar los servicios de terceros. Los términos contractuales se basan en formatos estandarizados. El riesgo del negocio asociado con los servicios del tercero está valorado y reportado.

DS3 Administrar el Desempeño y la Capacidad

Objetivo de control		Control a efectuar	Instrumentos aplicados	Documentación a revisar	Resultado
Subdominio	**Contenido**				
DS3.5 Monitoreo y Reporte	Monitorear continuamente el desempeño y la capacidad de los recursos de TI. La información reunida sirve para dos propósitos: • Mantener y poner a punto el desempeño actual dentro de TI y atender temas como elasticidad, contingencia, cargas de trabajo actuales y proyectadas, planes de almacenamiento y adquisición de recursos. • Para reportar la disponibilidad hacia el negocio del servicio prestado como se requiere en los SLAs. Acompañar todos los reportes de excepción con recomendaciones para acciones correctivas	Revisión documental. Entrevista a la Administradora de sistemas.	Cuestionarios. Observación.	Bitácoras.	Mediante el uso de las bitácoras se controla el desempeño y capacidades de los recursos. Existe una bitácora especial que sirve para para el registro de errores en los datos y las inconsistencias presentadas y así por ejemplo poder depurar la información o limpiar la base de datos, entre otras.

Modelo de madurez

DS3 Administrar el Desempeño y la Capacidad

La administración del proceso de Administrar el desempeño y la capacidad que satisfaga el requerimiento de optimizar el desempeño de la infraestructura, los recursos y las capacidades de TI, en respuesta a las necesidades de negocio es:

4 Administrado y Medible cuando

Hay procesos y herramientas disponibles para medir el uso del sistema, el desempeño y la capacidad, y los resultados se comparan con metas definidas. Hay información actualizada disponible, brindando estadísticas de desempeño estandarizadas y alertando sobre incidentes causados por falta de desempeño o de capacidad. Los problemas de falta de desempeño y de capacidad se enfrentan de acuerdo con procedimientos definidos y estandarizados. Se utilizan herramientas automatizadas para monitorear recursos específicos tales como espacios en disco, redes, servidores y compuertas de red. Las estadísticas de desempeño y capacidad son reportadas en términos de los procesos de negocio, de forma que los usuarios y los clientes comprendan los niveles de servicio de TI.

Los usuarios se sienten por lo general satisfechos con la capacidad del servicio actual y pueden solicitar nuevos y mejores niveles de disponibilidad. Se han acordado los KGIs y KPIs para medir el desempeño y la capacidad de TI, pero puede ser que se aplican de forma esporádica e inconsistente.

DS4 Garantizar la Continuidad del Servicio

Objetivo de control		Control a efectuar	Instrumentos aplicados	Documentación a revisar	Resultado
Subdominio	**Contenido**				
DS4.2 Planes de Continuidad de TI	Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.	Entrevista a la Administradora de sistemas.	Entrevista. Revisión documental.	Planes de continuidad.	En la cooperativa existen planes de continuidad en el área de sistemas para asegurar la continuidad del trabajo, sin embargo, no se pueden cumplir por falta de presupuesto para adquirir el hardware firewall necesario. Falta de decisión de mantener la plataforma actual o cambiar a una nueva.
DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones	Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio. El contenido de los respaldos a almacenar debe determinarse en conjunto entre los	Entrevista a la Administradora de sistemas.	Entrevista. Observación.		Actualmente todos los respaldos, documentación y otros recursos considerados como prioritarios se guardan en la bóveda de la cooperativa. Sin embargo, actualmente se están llevando a cabo las

	responsables de los procesos de negocio y el personal de TI. La administración del sitio de almacenamiento externo a las instalaciones, debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la empresa. La gerencia de TI debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos una vez por año, respecto al contenido, a la protección ambiental y a la seguridad. Asegurarse de la compatibilidad del hardware y del software para poder recuperar los datos archivados y periódicamente probar y renovar los datos archivados.				contrataciones necesarias para alquilar una bóveda en un Banco con el cuál la cooperativa ya mantiene otros acuerdos.

Modelo de madurez

DS4 Garantizar la Continuidad del Servicio

La administración del proceso de Garantizar la continuidad del servicio que satisfaga el requerimiento de TI del negocio para asegurar el mínimo impacto al negocio en caso de interrupción de un servicio de TI es:

4 Administrado y Medible cuando

Se hacen cumplir las responsabilidades y los estándares para la continuidad de los servicios. Se asigna la responsabilidad de mantener un plan de continuidad de servicios. Las actividades de mantenimiento están basadas en los resultados de las pruebas de continuidad, en las buenas prácticas internas y en los cambios en el ambiente del negocio y de TI. Se recopila, analiza y reporta documentación estructurada sobre la continuidad en los servicios y se actúa en consecuencia. Se brinda habilitación formal y obligatoria sobre los procesos de continuidad. Se implementan regularmente buenas prácticas de disponibilidad de los sistemas. Las prácticas de disponibilidad y la planeación de la continuidad de los servicios tienen influencia una sobre la otra. Se clasifican los incidentes de discontinuidad y la ruta de escalamiento es bien conocida por todos los involucrados. Se han desarrollado y acordado KGIs y KPIs para la continuidad de los servicios, aunque pueden ser medidos de manera inconsistente.

DS5 Garantizar la Seguridad de los Sistemas

Objetivo de control		Control a efectuar	Instrumentos aplicados	Documentación a revisar	Resultado
Subdominio	**Contenido**				
DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad	Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención.	Entrevista a la Administradora de sistemas. Revisión documental.	Entrevista. Observación	Bitácoras. Políticas de seguridad.	El acceso a los equipos está restringido mediante clave personal. El ingreso al sistema institucional está protegido por clave que debe ser cambiada cada 30 días de manera obligatoria.
DS5.9 Prevención, Detección y Corrección de Software Malicioso	Poner medidas preventivas, detectivas y correctivas (en especial contar con parches de seguridad y control de virus actualizados) en toda la organización para proteger los	Entrevista a la Administradora de sistemas. Revisión documental.		Bitácoras. Políticas de seguridad.	Existe un control adecuado de la seguridad lógica de los equipos, los mismos poseen protección del software antivirus Kaspersky Endpoint Security 10 que está instalado en red para todos los equipos de los usuarios finales,

	sistemas de la información y a la tecnología contra malware (virus, gusanos, spyware, correo basura).				además está instalado el software Agente de red Kaspersky Security Center que proporciona la comunicación entre el Servidor de Administración y el software antivirus de Kaspersky Lab. instalado en un nodo de red (estación de trabajo o servidor); el control de los mismos se lo realiza de manera centralizada desde el departamento de sistemas mediante el Paquete de red Kaspersky Security Center.
DS5.10 Seguridad de la Red	Uso de técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.	Entrevista a la Administradora de sistemas. Revisión documental.		Bitácoras. Políticas de seguridad.	Existe un firewall lógico instalado aunque el departamento de sistemas ha solicitado presupuesto para uno físico de la familia SOPHOS, pero por falta de apoyo no se ha podido implementar. La infraestructura de red instalada actualmente funciona adecuadamente, sin embargo es muy antigua por lo cual la Administradora de red ha pedido su cambio, pero no se ha realizado ya que la cooperativa mantiene planes de reconstrucción del edificio, mismos que no se han ejecutado por lo cual se pedirá nuevamente el cambio de la infraestructura.

Modelo de madurez

DS5 Garantizar la Seguridad de los Sistemas

La administración del proceso de Garantizar la seguridad de los sistemas que satisfaga el requerimiento de negocio de TI de mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad es:

4 Administrado y Medible cuando

Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. Regularmente se lleva a cabo un análisis de impacto y de riesgos de seguridad. Las políticas y prácticas de seguridad se complementan con referencias de seguridad específicas. El contacto con métodos para promover la conciencia de la seguridad es obligatorio. La identificación, autenticación y autorización de los usuarios está estandarizada. La certificación en seguridad es buscada por parte del personal que es responsable de la auditoría y la administración de la seguridad. Las prueba s de seguridad se hacen utilizando procesos estándares y formales que llevan a mejorar los niveles de seguridad. Los procesos de seguridad de TI están coordinados con la función de seguridad de toda la organización. Los reportes de seguridad están ligados con los objetivos del negocio. La habilitación sobre seguridad se imparte tanto para TI como para el negocio. La habilitación sobre seguridad de TI se planea y se administra de manera que responda a las necesidades del negocio y a los perfiles de riesgo de seguridad. Los KGIs y KPIs ya están definidos pero no se miden aún.

DS11 Administración de Datos

Objetivo de control		Control a efectuar	Instrumentos aplicados	Documentación a revisar	Resultado
Subdominio	**Contenido**				
DS11.2 Acuerdos de Almacenamiento y Conservación	Definir e implementar procedimientos para el archivo, almacenamiento y retención de los datos, de forma efectiva y eficiente para conseguir los objetivos de negocio, la política de seguridad de la organización y los requerimientos regulatorios.	Entrevista a la Administradora de sistemas. Revisión documental.	Entrevista Cuestionario Observación	Procedimientos de respaldo de información	Los procedimientos de respaldo de datos e información usados cumplen con los criterios de seguridad de la organización y leyes generales, además que ayudan a cumplir con los objetivos planteados por la entidad.

Modelo de madurez

DS11 Administración de Datos

La administración del proceso de Administrar los datos que satisfaga el requerimiento de negocio de TI de optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera es:

4 Administrado y Medible cuando

Se entiende la necesidad de la administración de los datos y las acciones requeridas son aceptadas a lo largo de toda la organización.

La responsabilidad de la propiedad y la administración de los datos están definidas, asignada y comunicada de forma clara en la organización. Los procedimientos se formalizan y son ampliamente conocidos, el conocimiento se comparte. Comienza a aparecer el uso de herramientas. Se acuerdan con los clientes los indicadores de desempeño y meta y se monitorean por medio de un proceso bien definido. Se lleva a cabo entrenamiento formal para el personal de administración de los datos.

DS12 Administración del Ambiente Físico

Objetivo de control		Control a efectuar	Instrumentos aplicados	Documentación a revisar	Resultado
Subdominio	**Contenido**				
DS12.2 Medidas de Seguridad Física	Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al esquema del perímetro de seguridad, de las zonas de seguridad, la ubicación de equipo crítico y de las áreas de envío y recepción. En particular, mantenga un perfil bajo respecto a la presencia de operaciones críticas de TI. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física.	Entrevista a la Administradora de sistemas. Revisión documental.	Entrevista. Observación Cuestionario Experimentación	Políticas de seguridad física.	Los equipos están inventariados y se actualizan constantemente. Los equipos están asegurados con Alianza Compañía se seguros y reaseguros S.A. Se cuenta con personal de seguridad contratado externamente. Existe un circuito de cámaras con operación centralizada que cubre la mayoría del espacio físico de la entidad interno y externo. Cada usuario es responsable por los equipos que le han sido cedidos para que cumpla con sus labores.
DS12.3 Acceso Físico	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a	Entrevista a la Administradora	Entrevista. Observación	Políticas de seguridad física.	En general existen políticas para el manejo y asesoría de personas externas, pero los mismos no se

	locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona.	de sistemas. Revisión documental.	Cuestionario Experimentación		cumplen a satisfacción. El departamento de sistemas recibe a los requerimientos de los socios en sus instalaciones, situación que no debería ser así ya que ésta se considera un área restringida para personas externas; ésto se lo realiza por falta de personal y detalle en los procesos documentados.
DS12.4 Protección Contra Factores Ambientales	Diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipo especializado para monitorear y controlar el ambiente.	Entrevista a la Administradora de sistemas. Revisión documental.	Entrevista. Observación Cuestionario	Políticas de seguridad física.	No existen medidas exclusivas para protección contra factores ambientales.

Modelo de madurez

DS12 Administración del Ambiente Físico

La administración del proceso de Administrar el ambiente físico que satisface el requerimiento del negocio de TI de proteger los activos de TI y la información del negocio y minimizar el riesgo de interrupciones en el negocio es:

3 Definido cuando

Se entiende y acepta a lo largo de toda la organización la necesidad de mantener un ambiente de cómputo controlado. Los controles ambientales, el mantenimiento preventivo y la seguridad física cuentan con presupuesto autorizado y rastreado por la gerencia. Se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo sólo al personal aprobado. Los visitantes se registran y acompañan dependiendo del individuo. Las instalaciones físicas mantienen un perfil bajo y no son reconocibles de manera fácil. Las autoridades civiles monitorean al cumplimiento con los reglamentos de salud y seguridad.

ME2 Monitorear y Evaluar el Control Interno

Objetivo de control		Control a efectuar	Instrumentos aplicados	Documentación a revisar	Resultado
Subdominio	**Contenido**				
ME2.1 Monitoreo del Marco de Trabajo de Control Interno	Monitorear de forma continua, comparar y mejorar el ambiente de control de TI y el marco de trabajo de control de TI para satisfacer los objetivos organizacionales.	Entrevista a la Administradora de sistemas. Revisión documental.	Entrevista. Observación	Medidas de control interno.	Las TI son controladas constantemente y se emite informes de su estado y sirven para poder medir y diagnosticar el estado del control interno y poder cumplir los objetivos organizacionales.
ME2.2 Revisiones de Auditoría	Monitorear y evaluar la eficiencia y efectividad de los controles internos de revisión de la gerencia de TI.	Entrevista a la Administradora de sistemas. Revisión documental.	Entrevista. Observación	Medidas de control interno.	El sistema institucional emite informes de auditoría en caso de ser necesarios, los mismos han permitido hasta la fecha tener una baja incidencia de problemas.
ME2.5 Aseguramiento del Control Interno	Obtener, según sea necesario, aseguramiento adicional de la completitud y efectividad de los controles internos por medio de revisiones de terceros.	Entrevista a la Administradora de sistemas. Revisión documental.	Entrevista. Observación	Medidas de control interno.	Ha habido una auditoría externa de la Superintendencia de Economía Popular y Solidaria en el mes de abril pero no han entregado los resultados.
ME2.7 Acciones Correctivas	Identificar, iniciar, rastrear e implementar acciones correctivas derivadas de los controles de evaluación y los informes.	Entrevista a la Administradora de sistemas.	Entrevista. Observación	Medidas de control interno.	No existe.

Modelo de madurez

ME2 Monitorear y Evaluar el Control Interno

La administración del proceso de Monitorear y evaluar el control interno que satisfaga el requerimiento de negocio de TI de proteger el logro de los objetivos de TI y cumplir con las leyes y regulaciones relacionadas con TI es:

3 Definido cuando

La gerencia apoya y ha institucionalizado el monitoreo del control interno. Se han desarrollado políticas y procedimientos para evaluar y reportar las actividades de monitoreo del control interno. Se ha definido un programa de educación y entrenamiento para el monitoreo del control interno. Se ha definido también un proceso para auto-evaluaciones y revisiones de aseguramiento del control interno, con roles definidos para los responsables de la administración del negocio y de TI. Se usan herramientas, aunque no necesariamente están integradas en todos los procesos. Las políticas de evaluación de riesgos de los procesos de TI se utilizan dentro de los marcos de trabajo desarrollados de manera específica para la función de TI. Se han definido políticas para el manejo y mitigación de riesgos específicos de procesos.

4.2.2.2.4 Diagrama del círculo de evaluación

Con esta herramienta de apoyo para la evaluación de los sistemas computacionales se puede valorar, visualmente, el comportamiento de los aspectos de los sistemas que están siendo auditados, así como su cumplimiento y limitaciones. Para lo cual primero se realizará la siguiente tabla recopilatoria:

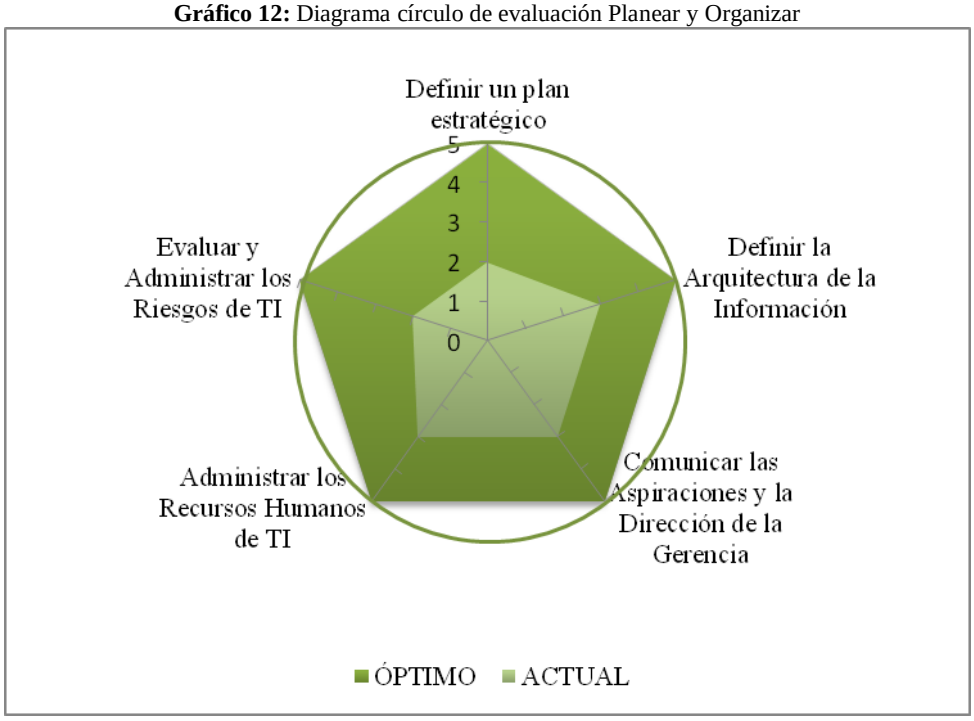
Cuadro 18: Matriz de grados de madurez

Matriz de Grados de Madurez		
Dominios y Subdominios		**Nivel de Madurez**
PLANEAR Y ORGANIZAR		**3***
PO1	Definir un plan estratégico	2
PO2	Definir la Arquitectura de la Información	3
PO6	Comunicar las Aspiraciones y la Dirección de la Gerencia	3
PO7	Administrar los Recursos Humanos de TI	3
PO9	Evaluar y Administrar los Riesgos de TI	2
ADQUIRIR E IMPLEMENTAR		**3***
AI2	Adquirir y Mantener Software Aplicativo	3
AI3	Adquirir y Mantener Infraestructura Tecnológica	4
AI4	Facilitar la Operación y el Uso	3
AI5	Adquirir Recursos de TI	3
AI6	Administrar cambios	5
ENTREGAR Y DAR SOPORTE		**4***
DS1	Definir y Administrar los Niveles de Servicio	3
DS2	Administrar los Servicios de Terceros	3
DS3	Administrar el Desempeño y la Capacidad	4
DS4	Garantizar la Continuidad del Servicio	4
DS5	Garantizar la Seguridad de los Sistemas	4
DS11	Administración de Datos	4
DS12	Administración del Ambiente Físico	3
MONITOREAR Y EVALUAR		**3***
ME2	Monitorear y Evaluar el Control Interno	3
* El valor obtenido es producto de aplicar la moda a los resultados obtenidos anteriormente.		

FUENTE: Análisis de subdominios
ELABORADO POR: Autor

Planear Y Organizar

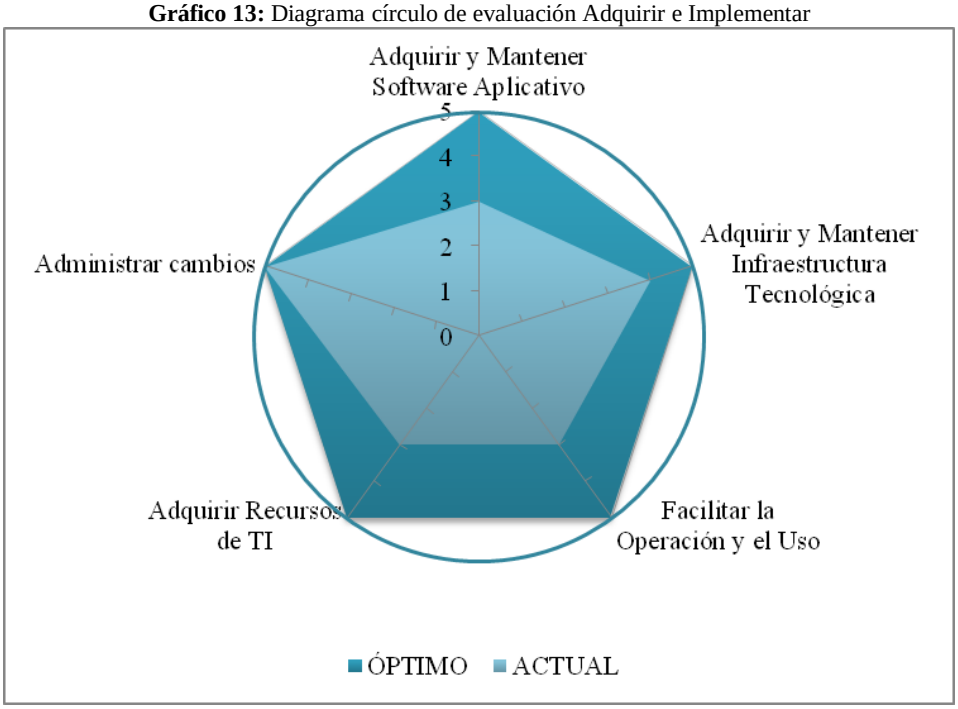
Gráfico 12: Diagrama círculo de evaluación Planear y Organizar



FUENTE: Análisis de subdominios
ELABORADO POR: Autor

Adquirir E Implementar

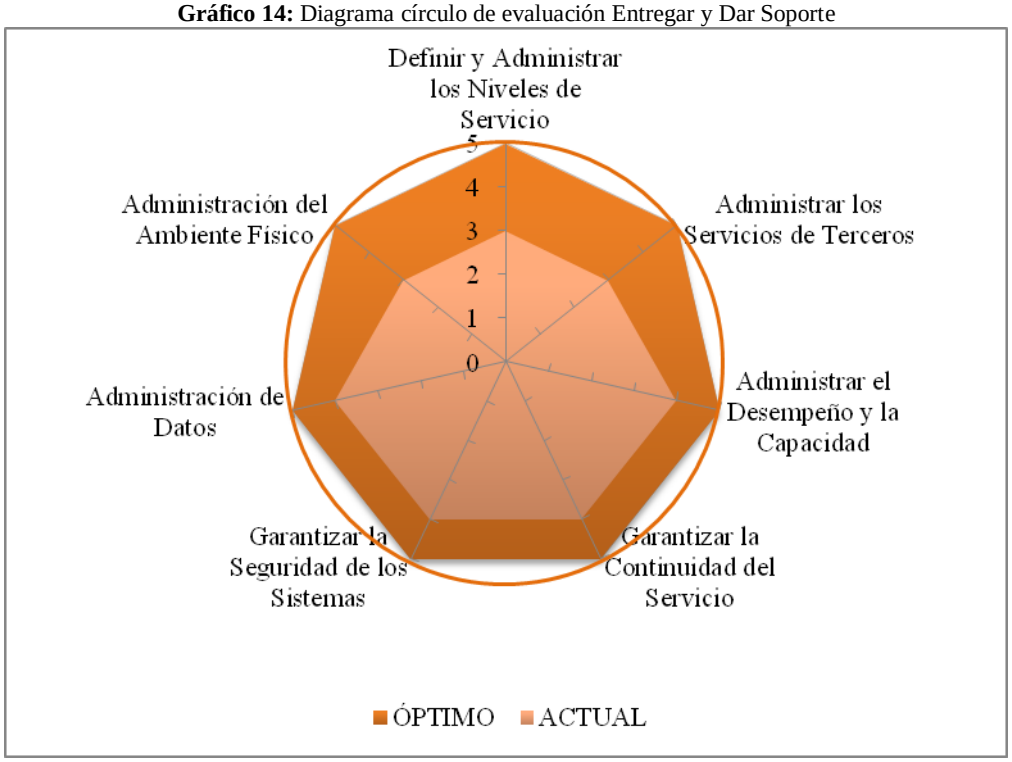
Gráfico 13: Diagrama círculo de evaluación Adquirir e Implementar



FUENTE: Análisis de subdominios
ELABORADO POR: Autor

Entregar Y Dar Soporte

Gráfico 14: Diagrama círculo de evaluación Entregar y Dar Soporte



FUENTE: Análisis de subdominios
ELABORADO POR: Autor

Monitorear Y Evaluar

No se puede construir una gráfica ya que solo se ha tomado un subdominio en ésta sección y no es suficiente ya que al menos se necesitan tres de los mismos.

4.2.2.3 Informe de la auditoría

4.2.2.3.1 Determinación de hallazgos

	HOJA DE HALLAZGOS	**HH 1/11**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

Título
Ausencia de un plan de capacitación contínuo para el manejo de las TIC.

Condición
No existe un plan de capacitación contínuo sobre el uso de las TIC para el personal.

Criterio
La Norma ISO 27002 en el punto **8.2.2. Formación y capacitación en seguridad de la información** expresa que: Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.

Causa
No se ha considerado dentro de los planes de operación de la entidad.

Efecto
Todo lo que conoce el personal administrativo y operacional sobre su uso y mantenimiento es producto de la inducción que reciben al iniciar sus actividades así como de su propia experiencia.

Elaborado por: EGMA	**Fecha:** 2015-10-12
Revisado por: VSHB	**Fecha:** 2015-10-12

	HOJA DE HALLAZGOS	**HH 2/11**

Entidad: CACECH
Naturaleza del trabajo: Auditoría de Sistemas Informáticos.
Período: Año 2014

Título
Manuales de funciones no alineados a TI para la organización.

Condición
Existen manuales de funciones establecidos para la administración, donde se detallan las funciones y atribuciones de los empleados, los mismos han sido desarrollados conforme a la política de seguridad de la entidad, pero no contemplan planes ni roles exclusivos para las TI.

Criterio
La Norma ISO 27002 expresa los siguientes puntos:
5.1.2 Revisión de la política de seguridad de la información: La política de seguridad de la información se debería revisar a intervalos planificados (o en caso que se produzcan cambios significativos) para garantizar que es adecuada, eficaz y suficiente.
6.1.1. Compromiso de la Dirección con la Seguridad de la Información expresa que: Los miembros de la Dirección deberían respaldar activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la Organización.
8.1.1. Inclusión de la seguridad en las responsabilidades laborales: Se deberían definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización.

Causa
No se han considerado las TI para desarrollar los manuales de funciones de la organización.

Efecto
No se puede analizar la manera en que el uso de las TI aporta al cumplimiento de los objetivos de la cooperativa, los señores empleados no saben cómo aportan o podrían aportar al mejor uso de las tecnologías y en la adquisición de futuros equipos para su trabajo.

Elaborado por: EGMA	**Fecha:** 2015-10-12
Revisado por: VSHB	**Fecha:** 2015-10-12

	HOJA DE HALLAZGOS	**HH 3/11**

Entidad:	CACECH
Naturaleza del trabajo:	Auditoría de Sistemas Informáticos.
Período:	Año 2014

Título

Inexistencia de un Marco de Trabajo de Administración de Riesgos de TI.

Condición

No existe un marco de trabajo de administración de riesgos de TI.

Criterio

La Norma ISO 27002 expresa los siguientes puntos:

14.1.1. Proceso de la gestión de continuidad del negocio: Se debería desarrollar y mantener un proceso de gestión de la continuidad del negocio en la organización que trate los requerimientos de seguridad de la información necesarios para la continuidad del negocio.

14.1.2. Continuidad del negocio y análisis de impactos: Se deberían identificar los eventos que puedan causar interrupciones a los procesos de negocio junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información.

Causa

No se ha considerado necesario por parte de la organización desarrollar un Marco de Trabajo exclusivo para la Administración de Riesgos de TI.

Efecto

La administradora del departamento de sistemas ha tenido que desarrollar sus propios métodos de trabajo y documentación para contrarrestar los riesgos, provocando que la organización quede desprotegida en caso de ausentarse la misma.

Al no haber un marco de Administración de riesgos no se puede saber en qué medida un riesgo ha afectado o puede afectar al cumplimiento de las metas y objetivos de la cooperativa.

Elaborado por: EGMA	**Fecha:** 2015-10-12
Revisado por: VSHB	**Fecha:** 2015-10-12

	HOJA DE HALLAZGOS	**HH 4/11**

Entidad:	CACECH
Naturaleza del trabajo:	Auditoría de Sistemas Informáticos.
Período:	Año 2014

Título

Falta de seguimiento por parte de auditoría interna.

Condición

El auditor interno no solicita reportes de auditoría.

Criterio

La Norma ISO 27002 expresa los siguientes puntos:

10.10.1. Registro de incidencias: Se deberían producir y mantener durante un periodo establecido los registros de auditoria con la grabación de las actividades de los usuarios, excepciones y eventos de la seguridad de información, con el fin de facilitar las investigaciones futuras y el monitoreo de los controles de acceso.

15.3.1. Controles de auditoria de sistemas: Se deberían planificar y acordar cuidadosamente los requisitos y actividades de auditoría que impliquen comprobaciones en los sistemas en activo con objeto de minimizar el riesgo de interrupciones de los procesos de negocio.

Causa

El auditor interno no solicita reportes del departamento de sistemas (al momento de la evaluación se justificó esto manifestando que el encargado del mismo asumió el cargo hace poco tiempo).

Efecto

Auditoría interna no conoce la realidad del departamento de sistemas. No puede medir ni evaluar la medida en la cual éste departamento está cumpliendo sus metas, tareas asignadas o los problemas que han surgido y emitir el informe correspondiente.

La administradora de sistemas emite informes continuamente, los mismos están archivados y listos para su revisión.

Elaborado por: EGMA	**Fecha:** 2015-10-12
Revisado por: VSHB	**Fecha:** 2015-10-12

	HOJA DE HALLAZGOS	**HH 5/11**

Entidad:	CACECH
Naturaleza del trabajo:	Auditoría de Sistemas Informáticos.
Período:	Año 2014

Título

Infracción de contrato.

Condición

Se ha detectado que el proveedor AVMEI Cía. Ltda. no cumple a satisfacción el contrato, ya que no cumple a satisfacción con la cláusula de mantenimiento de los servidores que ha instalado.

Criterio

La Norma ISO 27002 expresa los siguientes puntos:

10.2.1. Prestación de servicios: Se debería garantizar que los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el acuerdo de entrega de servicio externo sean implementados, operados y mantenidos por la parte externa.

10.2.2. Monitorización y revisión de los servicios contratados: Los servicios, informes y registros suministrados por terceros deberían ser monitoreados y revisados regularmente, y las auditorias se deberían realizar a intervalos regulares.

Causa

El proveedor no se acerca a las dependencias de la cooperativa para cumplir con su parte del contrato.

No existe otro proveedor que brinde los mismos servicios en el territorio nacional, por tanto éste ha manifestado a los directivos y a la Administradora de sistemas que sus empleados no se dan abasto para servir a sus clientes.

Efecto

Nace el riesgo de posibles fallas en los equipos y en los sistemas, aunque la Administradora está en capacidad de solventar muchas de ellas, hay componentes en los cuales no puede intervenir por riesgo a perder la garantía del proveedor.

Elaborado por: EGMA	**Fecha:** 2015-10-12
Revisado por: VSHB	**Fecha:** 2015-10-12

	HOJA DE HALLAZGOS	**HH 6/11**

Entidad:	CACECH
Naturaleza del trabajo:	Auditoría de Sistemas Informáticos.
Período:	Año 2014

Título

Sin asignación de presupuesto y falta de decisión.

Condición

En la cooperativa existen planes en el área de sistemas para asegurar la continuidad del trabajo, sin embargo, no se pueden cumplir a satisfacción.

Criterio

La Norma ISO 27002 expresa los siguientes puntos:

14.1.3. Redacción e implantación de planes de continuidad: Se deberían desarrollar e implantar planes de mantenimiento o recuperación de las operaciones del negocio para asegurar la disponibilidad de la información en el grado y en las escalas de tiempo requerido, tras la interrupción o fallo de los procesos críticos de negocio.

Causa

Falta de presupuesto y falta de decisión.

Efecto

No se ha podido adquirir el hardware firewall solicitado por la Administradora de sistemas para mejorar la seguridad de la información. No sé conoce si se actualizará la plataforma actual o si se la cambiará.

Elaborado por: EGMA	**Fecha:** 2015-10-12
Revisado por: VSHB	**Fecha:** 2015-10-12

	HOJA DE HALLAZGOS	**HH 7/11**

Entidad:	CACECH
Naturaleza del trabajo:	Auditoría de Sistemas Informáticos.
Período:	Año 2014

Título

Problemas con la infraestructura de red.

Condición

Existe riesgo en la infraestructura de red instalada actualmente por la antigüedad de la misma y falta de un equipo de seguridad.

Criterio

La Norma ISO 27002 expresa los siguientes puntos:

10.6.1. Controles de red: Se deberían mantener y controlar adecuadamente las redes para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones que utilizan las redes, incluyendo la información en tránsito.

10.6.2. Seguridad en los servicios de red: Se deberían identificar e incluir, en cualquier acuerdo sobre servicios de red, las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, independientemente de que estos servicios sean provistos desde la propia organización o se contratan desde el exterior.

Causa

La cooperativa mantiene planes de reconstrucción del edificio que no se completan, además no se ha decidido la compra de equipos necesarios.

Efecto

La infraestructura de red instalada actualmente funciona adecuadamente, sin embargo es muy antigua y necesita actualización de manera prioritaria.

No se ha adquirido el hardware firewall SOPHOS que sistemas ha considerado necesario para incrementar la seguridad de la información y los sistemas en general.

Elaborado por: EGMA	**Fecha:** 2015-10-12
Revisado por: VSHB	**Fecha:** 2015-10-12

	HOJA DE HALLAZGOS	**HH 8/11**

Entidad:	CACECH
Naturaleza del trabajo:	Auditoría de Sistemas Informáticos.
Período:	Año 2014

Título

Riesgo en el departamento de sistemas.

Condición

El departamento de sistemas recibe a personas externas a la cooperativa para resolver problemas suscitados, sin que los mismos se registren y solo se identifican verbalmente.

Criterio

La Norma ISO 27002 expresa los siguientes puntos:

6.2.1. Identificación de los riesgos derivados del acceso de terceros: Se deberían identificar los riesgos a la información de la organización y a las instalaciones del procesamiento de información de los procesos de negocio que impliquen a terceros y se deberían implementar controles apropiados antes de conceder el acceso.

9.1.2. Controles físicos de entrada: Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado.

9.1.6. Áreas aisladas de carga y descarga: Se deberían controlar las áreas de carga y descarga con objeto de evitar accesos no autorizados y, si es posible, aislarlas de los recursos para el tratamiento de la información.

Causa

Falta de personal y de detalle en los manuales de funciones.

Efecto

Se están infringiendo las políticas de seguridad de la cooperativa.

Se pone en riesgo la infraestructura tecnológica instalada.

Elaborado por: EGMA	**Fecha:** 2015-10-12
Revisado por: VSHB	**Fecha:** 2015-10-12

	HOJA DE HALLAZGOS	**HH 9/11**

Entidad:	CACECH
Naturaleza del trabajo:	Auditoría de Sistemas Informáticos.
Período:	Año 2014

Título

Ausencia de medidas.

Condición

No existen medidas exclusivas para protección contra factores ambientales, a excepción

Criterio

La Norma ISO 27002 expresa los siguientes puntos:

9.1.4. Protección contra amenazas externas y del entorno: Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.

Causa

No se han implementado éste tipo de políticas.

Efecto

No existen medidas de seguridad en caso de flagelos o desastres naturales ni humanos.

Elaborado por: EGMA	**Fecha:** 2015-10-12
Revisado por: VSHB	**Fecha:** 2015-10-12

	HOJA DE HALLAZGOS	**HH 10/11**

Entidad:	CACECH
Naturaleza del trabajo:	Auditoría de Sistemas Informáticos.
Período:	Año 2014

Título

Control externo deficiente.

Condición

Ha habido una auditoría externa de la Superintendencia de Economía Popular y Solidaria a los sistemas en el mes de abril pero no han entregado los resultados.

Criterio

La Norma ISO 27002 expresa los siguientes puntos:

6.1.8. Revisión Independiente de la Seguridad de la Información: Se deberían revisar las prácticas de la Organización para la gestión de la seguridad de la información y su implantación (por ej., objetivos de control, políticas, procesos y procedimientos de seguridad) de forma independiente y a intervalos planificados o cuando se produzcan cambios significativos para la seguridad de la información.

15.3.1. Controles de auditoria de sistemas: Se deberían planificar y acordar cuidadosamente los requisitos y actividades de auditoría que impliquen comprobaciones en los sistemas en activo con objeto de minimizar el riesgo de interrupciones de los procesos de negocio.

Causa

Fallos en la comunicación de resultados por parte de la Superintendencia de Economía Popular y Solidaria.

Efecto

La cooperativa y el departamento de sistemas no conocen si deben rectificar procedimientos o mejorar alguno ya que no poseen algún patrón de referencia para hacerlo.

Elaborado por: EGMA	**Fecha:** 2015-10-12
Revisado por: VSHB	**Fecha:** 2015-10-12

	HOJA DE HALLAZGOS	**HH 11/11**

Entidad:	CACECH
Naturaleza del trabajo:	Auditoría de Sistemas Informáticos.
Período:	Año 2014

Título
Ausencia de informes.

Condición
Inexistencia de informes de control.

Criterio
La Norma ISO 27002 expresa los siguientes puntos:

5.1.2 Revisión de la política de seguridad de la información: La política de seguridad de la información se debería revisar a intervalos planificados (o en caso que se produzcan cambios significativos) para garantizar que es adecuada, eficaz y suficiente.

15.2.1. Conformidad con la política de seguridad: Los directivos se deberían asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente y cumplen con los estándares y políticas de seguridad.

Causa
No existe un delegado que elabore informes de ésta índole para la entidad.

Efecto
Todas las acciones correctivas se aplican según van apareciendo y no son obtenidos en base a un informe técnico.

Elaborado por: EGMA	**Fecha:** 2015-10-12
Revisado por: VSHB	**Fecha:** 2015-10-12

4.2.2.3.2 Presentación del informe final

a) Carta de presentación

Riobamba, 16 de octubre del 2015
Ingeniero
César Oña Mendoza
Gerente General CACECH
Presente

De mi consideración

Se ha realizado la Auditoria Informática a la Facultad de la Cooperativa que usted gerencia muy acertadamente.

El análisis se realizó en base al marco de referencia COBIT 4.1 y las Normas ISO 27002, para el gobierno de las TI y poder verificar la existencia de desviaciones en los controles actuales.

A continuación se le presentará el respectivo informe con las conclusiones y recomendaciones del caso.

Atentamente

Michael Adrián Erazo Granizo
Auditor ME Auditores Independientes

b) Informe final

Informe de Auditoría Informática CACECH

Parte Primera

Motivo del examen

El presente examen se lo realizó para verificar la situación actual en cuanto al uso y aprovechamiento de las TIC en la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo Ltda.", en la misma se evaluó los cuatro aspectos considerados por las normas COBIT 4.1 y son : Planear y Organizar, Adquirir e Implementar, Entregar y dar Soporte, Monitorear y Evaluar. Esto se aplicó a toda la infraestructura de sistemas de la entidad.

Objetivo General

- Elaborar una auditoría de sistemas informáticos en la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda., de la ciudad de Riobamba, provincia de Chimborazo para el período 2014 para dictaminar respecto a la economía, eficiencia y eficacia de la utilización de los recursos tecnológicos.

Objetivos específicos

- Estructurar un marco teórico referencial que contribuya al desarrollo de la presente investigación.

- Aplicar la norma COBIT 4.1 y la norma ISO 27002, a fin de detectar la existencia de vulnerabilidades en los recursos de tecnologías de la información.

- Emitir un informe mostrando las respectivas conclusiones y recomendaciones que permita a la gerencia y al personal tomar los correctivos pertinentes.

Alcance

Sistemas e infraestructura de la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda.

Base Legal

Se aplicará las siguientes normativas:

- Marco de referencia COBIT en su versión 4.1
- Normas ISO 27002

COOPERATIVA DE AHORRO Y CRÉDITO "EDUCADORES DE CHIMBORAZO" LTDA.

Misión

"Somos una Institución Financiera que promueve la iniciativa de ahorro e inversión en el magisterio para mejorar la condición de vida de los socios".

Visión

En el año 2013, la Cooperativa liderará un Grupo Corporativo y estratégico para enfrentar los desafíos del futuro como una de las primeras Cooperativas del magisterio ecuatoriano.

Principios

- Respetar a la persona humana.
- Prioridad del servicio a los clientes.
- Mejoramiento contínuo.

Valores institucionales personales

- Entusiasmo.
- Ética.
- Solidaridad.
- Liderazgo.
- Trabajo en equipo.
- Responsabilidad Social.

- Compromiso.

- Confianza.

- Integridad con eficiencia.

Valores institucionales empresariales

- Productividad.

- Creatividad e Innovación.

- Competitividad.

- Compromiso y cultura de trabajo en equipo.

- Profesionalismo.

- Integración.

- Sanidad, prudencia y transparencia financiera.

Parte Segunda

Hallazgos y recomendaciones pertinentes

PO. Planear y Organizar

Ausencia de un plan de capacitación contínuo para el manejo de las TIC.

Conclusiones: La cooperativa no posee planes de capacitación sobre el uso de las TI de manera periódica para sus empleados. Sólo se capacita al personal cada vez que se produce un cambio, se contrata personal nuevo o se adquiere nuevas tecnologías.

Recomendaciones:

- A la gerencia.

Establecer planes de capacitación continua y periódica para el personal que labora en la cooperativa a fin de mejorar el aprovechamiento de las tecnologías utilizadas para desempeñar el trabajo en la misma.

Solicitar asesoría del departamento de sistemas a fin de detectar las áreas que necesitan refuerzo o la entrega de nuevos conocimientos o actualizaciones.

- A la administradora de sistemas

Monitorear permanentemente mediante conversaciones, documentación o la observación aquellos puntos relacionados con el uso de los sistemas informáticos en las cuales el resto personal presenta dificultades de uso o se presentan inconsistencias y mediante un informe sugerir a la gerencia autorice la capacitación conjunta de los mismos.

Manuales de funciones no alineados a TI para la organización.

Conclusiones: Los manuales de funciones que tiene la cooperativa para su personal no han considerado primordial para el desarrollo de ésta documentación la relación con el uso de las TI a fin que se relacionen directamente con las metas y objetivos que persigue la entidad.

Recomendaciones:

- A la gerencia:

Planificar y asignar a quién o a quiénes corresponda el rediseño de los manuales de funciones actuales a fin de que los mismos se acoplen con los lineamientos para el uso de las TI que maneja el departamento de sistemas.

Inexistencia de un Marco de Trabajo de Administración de riesgos de TI.

Conclusiones: No existe un marco de trabajo de administración de riesgos de TI que permita manejar los riesgos con asertividad.

Recomendaciones:

- A la gerencia:

Planificar y asignar a quién o a quiénes corresponda la creación de un Marco de Trabajo de Administración de riesgos de TI a fin de mejorar la mitigación de riesgos que se puedan presentar en la cooperativa. Se deberá evaluar si se diseña interna o externamente según las necesidades.

- A la administradora de sistemas

Entregar a la gerencia un informe con los litados y posibles contenidos que deberá poseer el Marco de Trabajo de Administración de riesgos de TI para su revisión y posible aprobación. Así mismo entregar todos los documentos e información adicional que posea para mejorar la calidad del trabajo final.

AI. Adquirir e Implementar

Falta de seguimiento por parte de auditoría interna.

Conclusiones: El encargado del departamento de auditoría interna no solicita reportes al departamento de sistemas para evaluar su gestión o procedimientos.

Recomendaciones:

- Al auditor interno

Acercarse de manera periódica al departamento de sistemas y solicitar información pertinente a las actividades que allí se ejecutan para su evaluación. (**Nota:** Se ha manifestado que el auditor interno no ha estado mucho tiempo y que es probable que por ésta razón aún no se ha acercado).

Infracción de contrato.

Conclusiones: El proveedor AVMEI Cía. Ltda. no cumple a satisfacción el contrato que mantiene con la cooperativa ya que no realiza el mantenimiento sobre los equipos que ha instalado.

Recomendaciones:

- A la gerencia:

Exigir al proveedor AVMEI Cía. Ltda. que cumpla con los servicios estipulados en el contrato que mantienen o hacer efectivas las cláusulas de sanción que se hayan estipulado en el mismo.

DS. Entregar y Dar Soporte

Sin asignación de presupuesto y falta de decisión.

Conclusiones: No se han podido adquirir equipos firewall por falta de decisión de los directivos de entregar el presupuesto necesario y por falta de decisión de actualizar o no la plataforma actual.

Recomendaciones:

- A la gerencia

Apoyar la adquisición de los equipos solicitados por el departamento de sistemas para beneficio y seguridad de toda la institución.

Decidir si se actualizará o se mantendrá la plataforma institucional que se usa actualmente a fin de asegurar el cumplimiento de los planes de continuidad ya que se han visto interrumpidos.

- Al consejo de administración

Considerar la entrega del presupuesto necesario para la adquisición de los equipos si está dentro de las posibilidades de entidad hacerlo.

Decidir si se actualizará o se mantendrá la plataforma institucional que se usa actualmente a fin de asegurar el cumplimiento de los planes de continuidad ya que se han visto interrumpidos.

Riesgo en el departamento de sistemas.

Conclusiones: Al departamento de sistemas ingresan personas externas a la institución con el fin de que la Administradora de sistemas les resuelva los problemas que se les ha suscitado referentes a sus cuentas, la autorización para su ingreso que reciben es solamente verbal.

Recomendaciones:

- A la gerencia

Aplicar la normativa interna de la empresa de no permitir el ingreso a personal externo a la cooperativa al interior del departamento de sistemas con e fin de precautelar la seguridad de la información. En caso de ser necesario el ingreso de éstas personas establecer un sistema de registro por escrito y presentando documentos de identificación de las mismas.

- A la Administradora de sistemas

Seguir aplicando la metodología actual al recibir personas externas a la cooperativa (de no dejar solas a las personas en el departamento); y sugerir a la gerencia aplique medidas en base a los reglamentos internos que le permitan aumentar el nivel de seguridad en el departamento de sistemas.

Ausencia de medidas contra factores medio ambientales.

Conclusiones: La cooperativa no posee medidas contra posibles emergencias que se pudiesen suscitar a causa de la presencia de factores medio ambientales que afecten a las infraestructura física, equipos, etc.

Las medidas que existen solo han sido diseñadas para el cajero que está ubicado en los exteriores de la cooperativa.

Recomendaciones:

- A la gerencia

Designar a quién o a quiénes corresponda la ampliación de las medidas de protección que actualmente solo contemplan el cajero, a fin que las mismas se extiendan a toda la institución con su respectiva adecuación a cada ambiente, las mismas deben mencionar las medidas a realizar, los responsables y más detalles necesarios a fin de precautelar la seguridad de los equipos y de la información que maneja.

Control externo deficiente

Conclusiones: No ha habido auditorías externas significativas para los sistemas informáticos de la cooperativa.

La auditoría externa realizada por los organismos de control no ha arrojado ningún resultado para ayudar a mejorar el funcionamiento o mantenimiento de los sistemas informáticos.

Recomendaciones:

- A la gerencia

Sería plausible y lo más acertado que en la contratación de futuras auditorías externas a la cooperativa se contemple también la revisión a los sistemas informáticos a fin de detectar si existe o no algún tipo de medidas correctivas o mejorar la gestión de los sistemas en general.

ME. Monitorear y Evaluar

No existen informes de control interno periódicos.

Conclusiones: No existe una persona que realiza informes periódicos sobre el manejo y situación del control interno, por lo cual no se puede aplicar medidas correctivas sobre éstos y se las aplica conforme van apareciendo y se las soluciona en base a los conocimientos de la encargada.

Recomendaciones:

- A la gerencia

Sería plausible y lo más acertado que en la contratación de futuras auditorías externas a la cooperativa se contemple también la revisión a los sistemas informáticos a fin de detectar si existe o no algún tipo de medidas correctivas o mejorar la gestión de los sistemas en general.

Ausencia de informes de control interno

Conclusiones: No se emiten informes de control interno de manera periódica que sirvan como base para la corrección de fallos en los procedimientos, trabajos o cualquier otra eventualidad.

Recomendaciones:

- A la gerencia

Designar a un delegado para la cooperativa o a uno de cada área la emisión de reportes cada cierto período de tiempo a fin que se obtenga información actualizada de los diferentes procesos que se llevan en la cooperativa y así puedan encaminarse conforme a los lineamientos de las TI.

- A la Administradora de sistemas

Solicitar a la gerencia, se sirva autorizar o delegar a quién corresponda que se le entreguen informes de control interno a fin que pueda adecuar su trabajo y tomar decisiones en base a los mismos.

Parte Tercera

Convocatoria lectura informe

Ingeniero
César Oña Mendoza
Gerente General CACECH
De mi consideración

De conformidad con lo establecido en el contrato de servicios que se firmó por mutuo acuerdo de las partes para iniciar la presente auditoría me permito comunicarle que la misma ha culminado y se procederá a la lectura de los resultados obtenidos el día 23 de octubre del presente año, en las instalaciones de su cooperativa.

Atentamente

Michael Adrián Erazo Granizo
Auditor ME Auditores Independientes

CONCLUSIONES

- La aplicación de la presente auditoría de sistemas informáticos en la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda., ha permitido determinar el nivel de economía, eficiencia y eficacia en la utilización de los recursos tecnológicos que se utilizan para el cumplimiento de objetivos y la satisfacción de las necesidades de los socios de la misma.

- La estructuración de un marco teórico referencial ha contribuido a que el presente investigación se realice en base a un lineamiento específico (no improvisado) evitando desperdicio de recursos y de tiempo, además, asegurando que los resultados sean más fiables, lógicos, medibles y comparables.

- La aplicación del marco de referencia COBIT 4.1 para determinar los puntos a evaluar y la utilización de la norma ISO 27002 para determinar los criterios aplicables a solucionar los inconvenientes encontrados, implican que los correctivos sugeridos y aquellos que se apliquen posteriormente efectivamente ayudarán a mejorar la utilización y mantenimiento del software, hardware e infraestructura tecnológica en general de la cooperativa.

- Se ha comunicado a la parte interesada los resultados de la revisión a través de un informe, en el mismo se da a conocer los principales fallos detectados y a la vez se sugiere los correctivos que deberían aplicarse para su corrección, queda a disposición de los interesados la aplicación de dichos correctivos.

RECOMENDACIONES

- Contratar auditorías que contemplen la revisión de los sistemas informáticos propiedad de la Cooperativa de Ahorro y Crédito “Educadores de Chimborazo” Ltda., a fin de poder verificar periódicamente los niveles de economía, eficiencia y eficacia en la utilización de los recursos tecnológicos utilizados para el cumplimiento de sus tareas primordiales.

- Utilizar un marco de trabajo establecido y validado por organismos supervisores para que los mismos sirvan como referencia para la evaluación a los sistemas informáticos de la cooperativa de forma interna, además, sirva como respaldo para evaluaciones externas futuras.

- Adquirir y aplicar el marco de referencia COBIT 4.1 para facilitar la detección de los puntos que necesiten mejoras, así mismo, también búsquese adquirir la certificación ISO 27002 por parte de una empresa auditora autorizada, avalando así sus procesos de uso y mantenimiento del software, hardware y la infraestructura que posee la entidad.

- Aplicar las recomendaciones sugeridas a fin de mejorar y asegurar la calidad de los productos entregados a sus socios, además asegurando la seguridad y máximo aprovechamiento de sus equipos y la información que procesan.

BIBLIOGRAFÍA

Behar, D. (2008). *Metodología de la investigación.* Panamá: Shalom.

Costas Santos, J. (2011). *Seguridad y alta disponibilidad.* México: RA-MA.

Fernández, C. (2012). La norma ISO 27002 del Sistema de Gestión de la Seguridad de la Información. *Seguridad y Salud*, Madrid: 40-44.

Guachi, T. (2012). Norma de seguridad informática ISO 27002 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el departamento de sistemas de la Cooperativa de Ahorro y Crédito San Francisco Ltda. Ambato: UTA.

Hernández Hernández, E. (2000). *Auditoría informática: Un enfoque metodológico.* México.: Continental.

IT Governance Institute. (2007). *COBIT 4.1*. Rolling Meadows: IT Governance Institute.

Kuna, H. (2006). Asistente para la realización de auditoría de sistemas en organismos públicos o privados. Madrid: Sol90.

Ministerio de Poder Popular para Transporte Terrestre. (2012). *Diccionario técnico de auditoría.* Chacao: Ministerio de Poder Popular para Transporte Terrestre.

Piattini, M. G., & Del Peso, E. (2001). *Auditoría informática: Un enfoque práctico.* México: Alfaomega.

Quintuña, V. (Abril de 2012). Auditoría informática a la Superintendencia de Telecomunicaciones. Cuenca: Universidad Estatal de Cuenca.

Ramírez, F. (2007). *Introducción a la Programación.* México: Alfaomega.

Razo Muñoz, C. (2002). *Auditoría en sistemas computacionales.* México: Pearson Educación.

The standardization committee. (2013). *ISO/ICE 27002*. Winterthur: SNV Schweizerische Normen-Vereinigung.

Internet

Fernández Menta, A. (2003). Nuevo Marco COSO de la Gestión de Riesgos. Buenos Aires: Obtenido de https://www.iaia.org.ar/revistas/normaria/Normaria09.pdf

Wales, J. (2008). *Wikipedia.org*. Obtenido de https://es.wikipedia.org/wiki/Wikipedia.

Oficina de Comercio del Gobierno Británico. (2015). *Econocom osiatis*. Obtenido de http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php

ANEXOS

Anexo 1. Encuestas aplicadas a la Administradora de sistemas

a) SEGURIDAD LÓGICA

Cuadro 19: Análisis de encuesta de seguridad lógica

N.	Pregunta	Respuesta
1	¿Se auditan los sistemas en operación?	**Si**
2	¿Con que frecuencia?	**A diario**
3	¿Existen calves de acceso a los equipos?	**Si**
4	¿Existen claves de acceso al sistema?	**Si**
5	¿Los usuarios se identifican individualmente?	**Si**
6	¿Los usuarios del sistema pueden cambiar a voluntad su contraseña facilitada por defecto?	**No** (El sistema pide cambio cada 30 días)
7	¿Se limita el número de intentos fallidos para la autenticación en el sistema?	**Si** (3 veces máximo)
8	¿Existen ficheros de logs que registran los accesos a los recursos y los intentos de acceso no autorizados?	**Si**
9	¿Las contraseñas contienen mayúsculas, minúsculas, números y signos de puntuación?	**Si** (excepto signos de puntuación)
10	¿Las contraseñas tienen una longitud mínima requerida?	**Si**
11	¿Los usuarios cambian sus contraseñas, al menos, una vez cada 30 días o cuando sospechan que sus contraseñas han dejado de ser confidenciales?	**Si**
12	¿A todos los ficheros que contienen datos de carácter personal se les aplica, al menos, medidas de nivel básico?	**No se guardan archivos personales.**
13	¿Los usuarios tienen acceso únicamente a los recursos que necesitan para desempeñar su labor?	**Si** (La administradora solo habilita los módulos necesarios para cada empleado en el sistema)
14	¿Se revocan los derechos de acceso al sistema cuando los usuarios finalizan su actividad en la cooperativa?	**Si**

N.	Pregunta	Respuesta
15	¿Se han infectado en alguna ocasión, los equipos de la empresa con código malicioso?	**No**
16	¿Se utilizan programas antivirus para prevenir, detectar y eliminar malware?	**Si**
17	¿Se utiliza un cortafuegos bien configurado para actuar como filtro entre redes facilitando las comunicaciones autorizadas y evitando los accesos ilícitos?	**Si** (Es un cortafuegos lógico pero hace falta implementar otro físico que complemente e incremente la seguridad)
18	¿Se actualizan con frecuencia los programas dedicados a la detección y eliminación de código malicioso?	**Si** (De forma automática)
19	¿Se realizan pruebas para verificar que los mecanismos de seguridad funcionan correctamente?	**Si** (Se emite reporte semanal)
20	¿Los programas instalados en los equipos de la entidad utilizan licencias originales?	**Si**
21	¿Se instalan los parches y las últimas versiones de los programas usados en la cooperativa?	**Si**
22	¿Se han detectado programas de origen desconocido instalados en los equipos?	**No**
23	¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?	**No existe ya que se realiza una inmersión a los sistemas a los nuevos empleados.**

b) SEGURIDAD FÍSICA

Cuadro 20: Análisis de encuesta de seguridad física

N.	Pregunta	Respuesta
1	El edificio donde se encuentra la computadora está situado a salvo de:	**Inundación** (No se dijo que la construcción esté a salvo de terremotos, fuego o sabotaje) ✓
2	¿El centro de cómputo tiene salida directa al exterior?	**Si** ✓
3	Describa brevemente la construcción del centro de cómputo, de preferencia proporcionando planos y material con que construido y equipo (muebles, sillas etc.) dentro del centro.	**Se adecuó, ya que es una construcción antigua.** ✓
4	¿Existe control en el acceso a este cuarto?	**Con llaves** ✓
5	¿Son controladas las visitas o intervenciones en el centro de cómputo?	**Si** ✓
6	¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática?	**No** ✓ ‖
7	¿Se han adoptado medidas de seguridad en el departamento de sistemas?	**Si** ✓
8	¿Existen una persona responsable de la seguridad?	**Si** ✓
9	¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?	**Si** ✓
10	¿Existe personal de vigilancia en la institución?	**Si** ✓
11	¿La vigilancia se contrata?	**Por medio de empresas que venden el servicio.** ✓
12	¿Existe alarma para detectar?	**Fuego, Robo** (No existe otra alarma) ✓
13	¿Estas alarmas están?	**Cajero** ✓
14	¿Existe alarma para detectar condiciones anormales del ambiente?	**Cajero** ✓
15	¿La alarma es perfectamente audible?	**Si** ✓
16	Esta alarma también está conectada a:	**Empresa de vigilancia** ✓

N.	Pregunta	Respuesta	
17	¿Saben que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?	**Si**	✓
18	Existen extintores de fuego	**Si** (Manuales)	✓
19	¿Se ha adiestrado el personal en el manejo de los extintores?	**Si**	✓
20	Los extintores, manuales o automáticos a base de	**Espuma / polvo**	✓
21	¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?	**Si** (Lo realiza el Cuerpo de Bomberos)	✓
22	¿Se ha tomado medidas para que el material de los extintores no cause más daño que el fuego?	**Si**	✓
23	¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?	**Si**	✓
24	¿El personal ajeno a operación sabe qué hacer en el caso de una emergencia (incendio)?	**Si**	✓
25	¿Existe salida de emergencia?	**Si**	✓
26	Esta puerta se abre:	**Por ambos lados**	✓
27	¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?	**Si**	✓
28	Se ha tomado medidas para minimizar la posibilidad de fuego:	**Evitando artículos inflamables, Prohibiendo fumar a los operadores en el interior, Vigilando y manteniendo el sistema eléctrico**	✓
29	Explique la forma como se ha clasificado la información vital, esencial, no esencial etc.	**Vital → Base de datos, instaladores, claves, reportes Esencial → Información**	✓

N.	Pregunta	Respuesta
30	¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?	**Si** ✓
31	¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?	**Si** ✓
32	Explique la forma en que están protegidas físicamente estas copias (bóveda, cajas de seguridad etc.) que garantice su integridad en caso de incendio, inundación, terremotos, etc.	**La cooperativa tiene una bóveda propia, aunque se planea llevarla fuera al Banco del Austro.** ✓
33	¿Si se tienen terminales conectadas, se ha establecido procedimientos de operación?	**Si** ✓
34	Se verifica identificación:	**De usuarios** ✓
35	¿Los equipos usados están conectados a una unidad que los proteja de variaciones de voltaje?	**Si** ✓
36	¿Los servidores de la cooperativa están debidamente protegidos?	**Si** ✓
37	¿Los cables de red están debidamente conectados y protegidos?	**No** (El cableado red es antigua/ Solo se cuenta con cableado estructurado en el segundo piso). ✓

c) Tecnologías de la Información y Comunicación

Cuadro 21: Análisis de encuesta de las TIC

N.	Pregunta	Respuesta	
1	¿La cooperativa tiene una intranet?	**No**	✓
2	¿La cooperativa dispone de servicio de internet?	**Si**	✓
3	¿Cuál es la velocidad de la conexión a internet que tiene contratada la cooperativa?	**1 Mb**	✓
4	El internet se distribuye:	**Mediante conexión cableada a todas las terminales y mediante WI-FI para backup.**	✓
5	Indique el nombre de su proveedor de internet	**Telconet / Puntonet**	✓
6	¿En caso de corte del servicio, el proveedor restablece el servicio de manera ágil?	**Si**	✓
7	¿La cooperativa se comunica a través de su cuenta de correo electrónico?	**Si**	✓
8	El correo electrónico que usa la cooperativa es:	**Genérico / Personalizado**	✓
9	¿Se tienen listados los correos electrónicos de los socios de la cooperativa?	**Si** (Se está actualizando el correo de todos los socios hasta fin de año).	✓ ©
10	¿La cooperativa tiene página web?	**Si**	✓
11	¿Se actualiza constantemente ésta página web?	**Si**	✓
12	¿Se ofertan servicios a través de la página web a los socios?	**Si**	✓
13	¿Se usa tecnología voIP para las comunicaciones telefónicas?	**No** (se usa el servicio de telefonía tradicional)	✓

d) Gestión informática

Cuadro 22: Análisis de encuesta a la gestión informática

N.	Pregunta	Respuesta
1	¿Existe una clara definición de funciones entre los puestos clave?	**Si**
2	¿Existe un sistema de captación de datos?	**Si**
3	¿Existen procedimientos formales para la operación del sistema de cómputo?	**Si**
4	Indique la periodicidad de la actualización de los procedimientos:	**Cada vez que haya cambios en los equipos.**
5	¿Existe un control que asegure la justificación de los procesos en el computador? (Que los procesos están autorizados y tengan una razón de ser procesados).	**Si**
6	¿Existen procedimientos escritos para la recuperación del sistema en caso de falla?	**Si**
7	¿Cómo se actúa en caso de errores?	**Se busca la causa y se trata de solucionar inmediatamente. De ser necesario se usa documentación pertinente.**
8	¿Existen instrucciones específicas para cada proceso, con las indicaciones pertinentes?	**Si** (La mayoría de los procesos las tienen).
9	¿Se tienen procedimientos específicos que indiquen al operador que hacer cuando un programa interrumpe su ejecución u otras dificultades en proceso?	**No**
10	¿Se prohíbe al operador modificar información de archivos?	**Si**
11	¿Se realiza funciones de mantenimiento periódico preventivo o correctivo en dispositivos que así lo requieran?	**Si**
12	¿Se llevan a cabo revisiones periódicas de los sistemas para determinar si cumplen con los objetivos para los cuales fueron adquiridos?	**Si**

N.	Pregunta	Respuesta
13	Las intervenciones de los operadores:	**Se limitan a lo esencial.**
14	¿Cómo controlan los trabajos dentro del departamento de cómputo?	**Mediante el uso de bitácoras.**
15	¿Cuentan los operadores con una bitácora para mantener registros de cualquier evento y acción tomada por ellos?	**Si**
16	¿Existe un registro de funcionamiento que muestre el tiempo de paros y mantenimiento o instalaciones de software?	**Si**
17	¿Existen procedimientos para evitar las corridas de programas no autorizados?	**Si** (A través del antivirus)
18	¿Existe un lugar para archivar los registros del sistema o equipo de cómputo?	**Si**
19	Si la respuesta anterior es positiva, indique como está organizado este archivo de bitácora.	**Por fecha y hora**
20	¿Se tiene inventario actualizado de los equipos y terminales con su localización?	**Si**
21	¿Se tienen seguros sobre todos los equipos?	**Si**
22	Si la respuesta anterior es positiva, indique la compañía de seguros.	**Alianza Seguros**
23	¿Qué se hace con la información utilizada y que ya no es útil?	**Se destruye**
24	¿Existe departamento de auditoria interna en la institución?	**Si**
25	¿Este departamento de auditoria interna conoce todos los aspectos de los sistemas?	**Si**
26	¿Se controla el trabajo fuera de horario?	**Si**
27	¿Se ha definido una política de seguridad en la cooperativa?	**Si**
28	¿La política de seguridad es coherente con la política de la cooperativa?	**Si**
29	¿La política de seguridad es conforme con los requisitos legales?	**Si**
30	¿La política de seguridad muestra un lenguaje entendible por todo el personal de la empresa?	**Si**
31	¿Se fomenta la comunicación de la política de seguridad?	**No**
32	¿La política de seguridad se cumple rigurosamente por todos los empleados de la cooperativa?	**No**
33	¿Existe en la empresa un responsable o responsables encargados del desarrollo, revisión y evaluación de la Política de Seguridad con la suficiente formación y experiencia?	**Si**

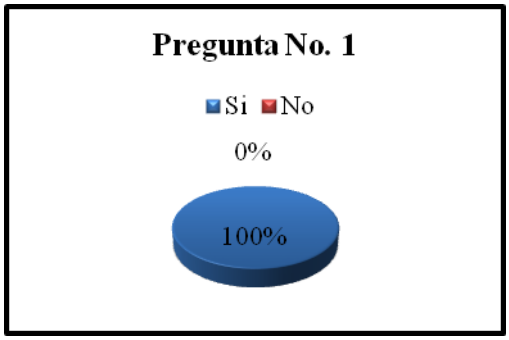
Anexo 2. Encuestas aplicadas al personal

Claves

1. ¿Sus claves de acceso al sistema son conocidas única y exclusivamente por usted?

Si	11	100,00%
No	0	0,00%
Total	11	100,00%

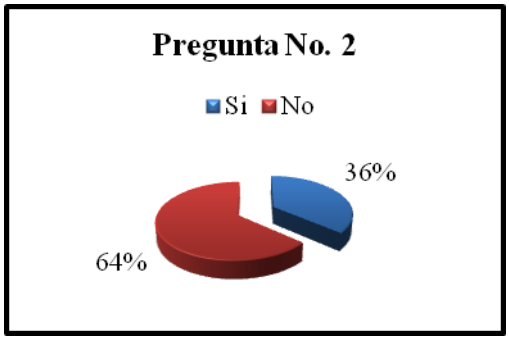
Fuente: Investigación
Elaborado por: Autor



2. ¿Conoce usted los métodos para establecer claves seguras?

Si	4	36,36%
No	7	63,64%
Total	11	100,00%

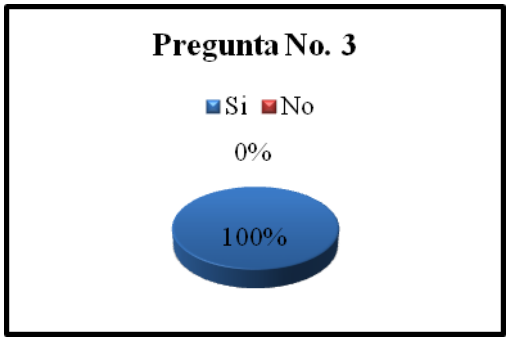
Fuente: Investigación
Elaborado por: Autor



3. ¿Le han indicado que hacer en caso de olvido o pérdida de sus claves?

Si	11	100,00%
No	0	0,00%
Total	11	100,00%

Fuente: Investigación
Elaborado por: Autor

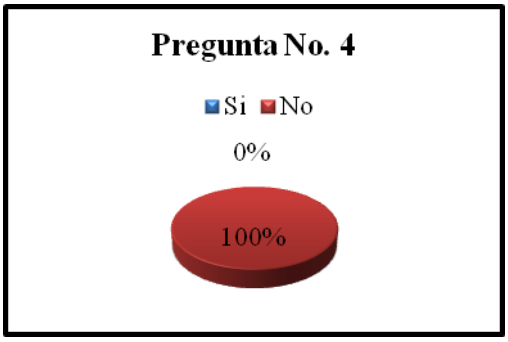


Fallos

4. ¿Ha tenido fallos del equipo informático mientras trabaja en él?

Si	0	100,00%
No	11	0,00%
Total	11	100,00%

Fuente: Investigación
Elaborado por: Autor



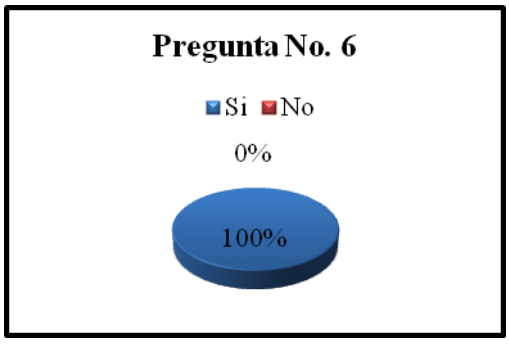
5. Si es así ¿Generalmente ha podido recuperar su trabajo de manera íntegra?

No aplica, ya que los equipos no han presentado fallos graves.

6. ¿Comunica usted de forma breve al departamento de sistemas cuando tiene problemas con los equipos?

Si	11	100,00%
No	0	0,00%
Total	11	100,00%

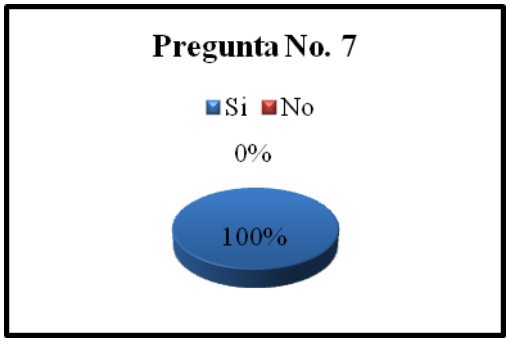
Fuente: Investigación
Elaborado por: Autor



7. ¿El departamento de sistemas atiende sus requerimientos de forma oportuna?

Si	11	100,00%
No	0	0,00%
Total	11	100,00%

Fuente: Investigación
Elaborado por: Autor

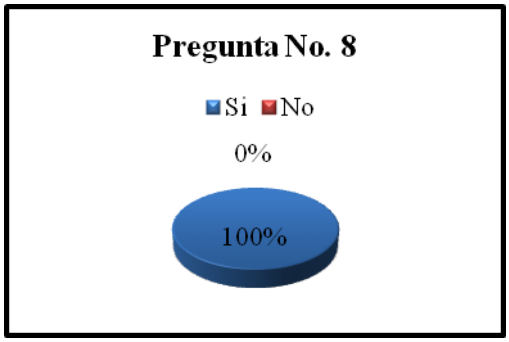


Seguridad

8. A su criterio ¿Cree que existen las seguridades adecuadas para evitar daños o alteraciones en los sistemas de la cooperativa?

Si	11	100,00%
No	0	0,00%
Total	11	100,00%

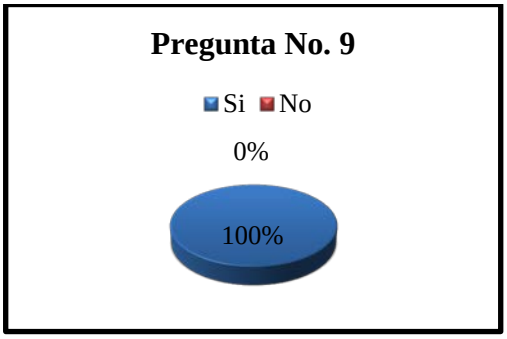
Fuente: Investigación
Elaborado por: Autor



9. ¿Conoce usted el procedimiento adecuado para eliminar archivos de su equipo para evitar el mal uso de la información ahí contenida?

Si	11	100,00%
No	0	0,00%
Total	11	100,00%

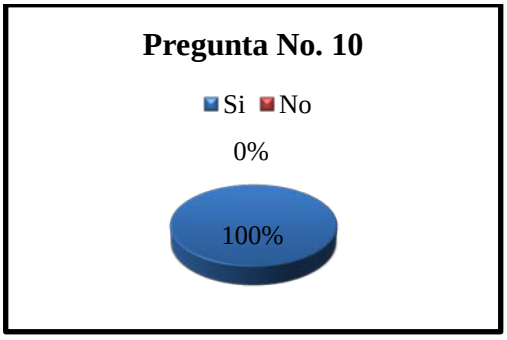
Fuente: Investigación
Elaborado por: Autor



10. ¿Cree usted que la información interna de la cooperativa está bien resguardada?

Si	11	100,00%
No	0	0,00%
Total	11	100,00%

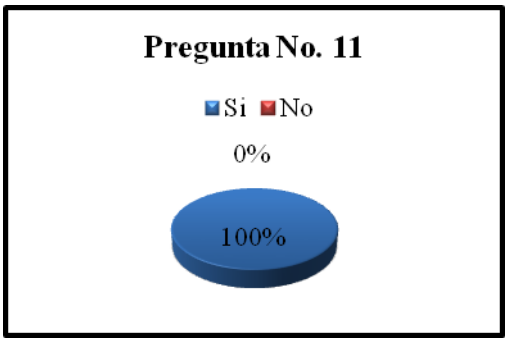
Fuente: Investigación
Elaborado por: Autor



11. ¿Cree usted que los equipos de la cooperativa están bien resguardados?

Si	11	100,00%
No	0	0,00%
Total	11	100,00%

Fuente: Investigación
Elaborado por: Autor

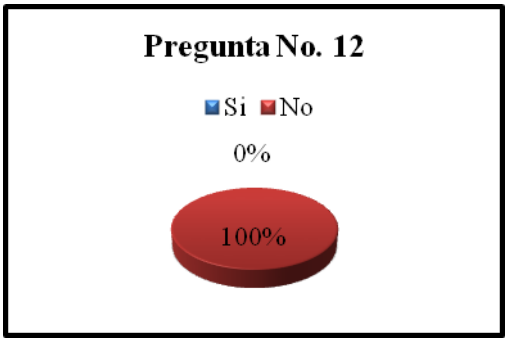


Procedimientos

12. ¿Se le ha entregado manuales de procedimientos o políticas de manejo de los equipos por escrito?

Si	0	0,00%
No	11	100,00%
Total	11	100,00%

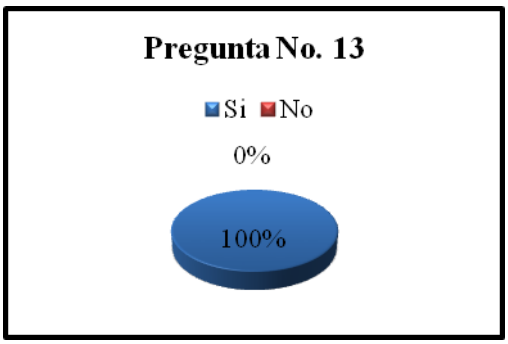
Fuente: Investigación
Elaborado por: Autor



13. ¿Considera usted qué el equipo que usa satisface los requerimientos necesarios para el desempeño de sus labores?

Si	11	100,00%
No	0	0,00%
Total	11	100,00%

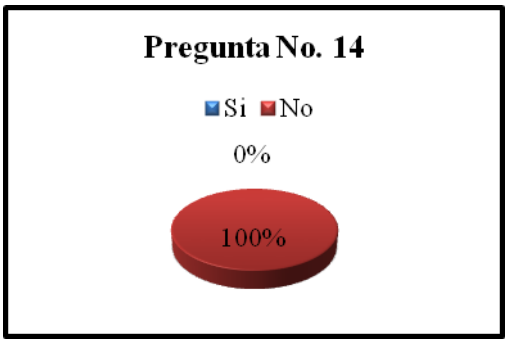
Fuente: Investigación
Elaborado por: Autor



14. ¿Conoce usted las políticas generales para el uso y operación de los equipos informáticos?

Si	0	0,00%
No	11	100,00%
Total	11	100,00%

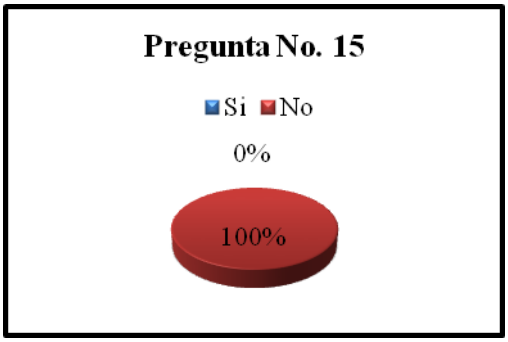
Fuente: Investigación
Elaborado por: Autor



15. ¿Conoce usted las políticas que se han establecido para el cambio de claves de acceso al sistema operativo, correo electrónico, otros sistemas?

Si	0	0,00%
No	11	100,00%
Total	11	100,00%

Fuente: Investigación
Elaborado por: Autor

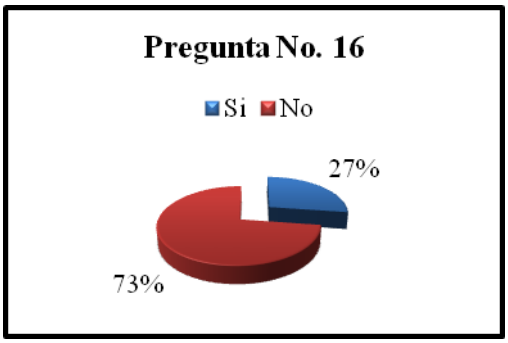


Respaldos

16. ¿Crea usted respaldos de la información y demás archivos con los que trabaja?

Si	3	27,27%
No	8	72,73%
Total	11	100,00%

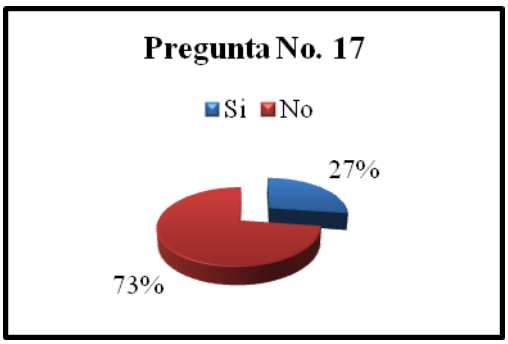
Fuente: Investigación
Elaborado por: Autor



17. ¿Guarda sus respaldos en un lugar seguro?

Si	3	27,27%
No	8	72,73%
Total	11	100,00%

Fuente: Investigación
Elaborado por: Autor



Anexo 3. Inventario de software

Cuadro 23: Inventario de software

N.	Nombre Software		Versiones instaladas	Licencias				
				Total	Original		Vigente	
					Si	No	Si	No
Software de aplicación								
1	Mozilla Firefox	14	40.0	**23**	**X**		**X**	
		1	12.0					
		1	3.0.19					
		4	37.0.1					
		2	3.0.1					
		1	8.3.60					
2	CONEXUS		5.1.0	**18**	**X**		**X**	
3	Compresor WinRAR		3.80	**17**	**X**		**X**	
4	WinZip		9.0	**15**	**X**		**X**	
5	Agente de red Kaspersky Security Center		10.2	**15**	**X**		**X**	
6	Informix		2.10	**14**	**X**		**X**	
7	Kaspersky Endpoint Security 10		10.2	**13**	**X**		**X**	
8	Microsoft Office Professinal Plus 2010		14.0	**13**	**X**		**X**	
9	Nero		8.3	**12**	**X**		**X**	
10	TeamViewer	1	7.0	**11**	**X**		**X**	
		9	8.0					
		1	10.0					
11	PARDUS		5.0.0	**10**	**X**		**X**	
12	Google Chrome		45.0	**9**	**X**		**X**	
13	DIMM		1.0.1	**8**	**X**		**X**	
14	doPDF		7.3	**8**	**X**		**X**	
15	Magical JellyBean KeyFinder		2.0.9	**7**	**X**		**X**	
16	Adobe Reader XI		11.0	**7**	**X**		**X**	
17	Microsoft Office Enterprise 2007		12.0	**7**	**X**		**X**	
18	Microsoft Office Project Professional 2007		12.0	**6**	**X**		**X**	
19	Skype	2	6	**6**	**X**		**X**	
		1	7.3					
		3	5.5					
20	Internet Explorer	1	10.0	**6**	**X**		**X**	
21		5	8					
22	Adobe Reader X		10.1	**5**	**X**		**X**	
23	Microsoft Office Visio Professional 2007		12.0	**5**	**X**		**X**	
24	Notepad++		6.6	**4**	**X**		**X**	

N.	Nombre Software	Versiones instaladas	Licencias				
			Número	Original		Vigente	
				Si	No	Si	No
25	Sistema de análisis crediticio RATIOS	2.2.0	4	X		X	
26	Adobe Reader IX	9.2	3	X		X	
27	CCleaner	3.26	3	X		X	
28	Microsoft SQL Server 2008		3	X		X	
29	Filezilla Client	3.10	3	X		X	
30	PDF Complete	3.5.22	3	X		X	
31	VLC Media Player	1.1	3	X		X	
32	Microsoft Office Access 2003 Runtime	11.0	2	X		X	
33	Microsoft Visual Studio 2010	10.0	2	X		X	
34	PEARLS	4.0.17	2	X		X	
35	Kaspersky Antivirus	6	2	X		X	
36	aTube Catcher	3.8	2	X		X	
37	DriverPack Solution Updater	0.0.25	2	X		X	
38	LighScribe Applications	1.18	2	X		X	
39	PGP Desktop	10.0	2	X		X	
40	Windows Media Reproductor		2	X		X	
41	Paquete de red Kaspersky Security Center	10.2	2	X		X	
42	Microsoft Office Professinal Plus 2007	12.0	1	X		X	
43	Microsoft Office Professinal Plus 2013	15.0	1	X		X	
44	Servidor de administración de Kaspersky Security	10.2	1	X		X	
45	Microsoft .NET Framework 4		1	X		X	
46	Evernote	4.2.3	1	X		X	
47	Genie Cleaner	9.0	1	X		X	
48	Genie Wifi	9.0	1	X		X	
49	Label Print	2.5	1	X		X	
50	Cyberlink DVD Suite	1	1	X		X	
51	Hulu Desktop	0.9.13	1	X		X	
52	Geovision GV250 Syslin		1	X		X	
53	ExamView Player		1	X		X	
54	iVMS	1.0	1	X		X	
55	Nero Burning ROM 2015	16.0	1	X		X	
56	Digital VoicerEditor	3	1	X		X	
57	AVI Generator	1.8	1	X		X	
58	Comodo Dragon	33.1	1	X		X	
59	Renderis Pro	14.0	1	X		X	
60	Sumatra PDF	3.0	1	X		X	

N.	Nombre Software	Versiones instaladas	Licencias				
			Número	Original		Vigente	
				Si	No	Si	No
61	Screenshot Captor	2.8	1	X		X	
62	DVD Shink		1	X		X	
63	OCR Software by I.R.I.S.		1	X		X	
64	Live Sync	14.5	1	X		X	
65	Web Companion		1	X		X	
66	Nokia Connectivity Cable Driver	1.1	1	X		X	
67	Readiris PRO	7.1.32	1	X		X	
68	Video downloader		1	X		X	
69	UltraCompare	11	1	X		X	
70	BlueJ	1.5	1	X		X	
71	Context	8.50	1	X		X	
72	Adobe Photoshop Elements		1	X		X	
73	Adobe Premier Elements		1	X		X	
74	NisSoft ProduKey		1	X		X	
75	PRTG Network Monitor	9	1	X		X	
76	Picasa	3.9	1	X		X	
77	7-Zip	4.65	1	X		X	
78	UltraCompare	8.50	1	X		X	
79	CinemaNow Media Manager		1	X		X	
80	Yonta	1.10	1	X		X	
81	Windows Live Essentials 2011	15.3	1	X		X	
82	Songr	20.0	1	X		X	
83	HashX	1.0.1	1	X		X	
84	Adobe Ilustrator CS3	3.0	1	X		X	
85	Adobe Photoshop CS3	3.0	1	X		X	
86	InterVideo WinDVD 8	8.2	1	X		X	
87	McAfee Security Scan Plus	3.54	1	X		X	
88	KMPlayer		1	X		X	
89	Learning Essentials para Microsoft Office		1	X		X	
90	LEC Power Translator		1	X		X	
91	LEC Translate	11	1	X		X	
92	Microsoft Office 2003 Web Components		1	X		X	
93	Microsoft Student con encarta Premium 2009		1	X		X	
94	Mobogenie	3	1	X		X	
95	PhotoScape	3.7	1	X		X	
96	SoundMax	5.2.0	1	X		X	

N.	Nombre Software		Versiones instaladas	Licencias				
				Número	Original		Vigente	
					Si	No	Si	No
97	Windows Live Essentials			1	X		X	
98	Altiris Software Virtualization Agent			1	X		X	
99	WinPcap		4.0.0	1	X		X	
Sistemas Operativos								
1	Windows 8 Pro		SP2	6	X		X	
2	Windows 7 Professional		SP1	6	X		X	
3	Windows 7 Home Premium		SP1	5	X		X	
4	Windows XP		SP3	4	X		X	
5	Centos 6 Server			2	X		X	
6	Windows 2003 Server Edition			1	X		X	
7	Windows 2008 Server Edition			1	X		X	
Drivers, aplicaciones en segundo plano								
1	Adobe Flash Player NPAPI	5	19.0	14	X		X	
		1	16.0					
		6	18.0					
		2	11.0					
2	Adobe Flash Player ActiveX	5	19.0	11	X		X	
		6	18.0					
3	Java	2	8	8	X		X	
		4	6					
		2	7					
4	Adobe Shockwave Player		12.0	5	X		X	
5	Java SE Development Kit		6	1	X		X	

Fuente: Toma física
Elaborador por: Autor

Anexo 4. Inventario de hardware

Cuadro 24: Inventario de hardware

Área	Usuario	Cargo	N.	Activo Fijo	Descripción	Marca	Serie	Estado Físico
Contabilidad	Hernández Vaca Verónica	Asistente 1	1	CPU	2 GB RAM / 253 GB HDD Procesador Intel i3 / 32 bits	HP	MXL039052R	Bueno
			2	Teclado	Latam. / Alfanumérico / USB	HP		Bueno
			3	Mouse	Láser / 3 botones / scroll / USB	HP		Bueno
			4	Monitor	Pantalla plana 18,0” LCD	HP	CNC013Q7BD	Bueno
			5	Impresora	LaserJet P2055dn / Monocrom.	HP	CN9053647	Bueno
	Carrillo R. Blanquita	Contadora	6	CPU	2 GB RAM / 465 GB HDD Procesador Intel i3 / 32 bits	HP	MXL0382C45	Regular
			7	Teclado	Latam. / Alfanumérico / USB	HP		Bueno
			8	Mouse	Láser / 3 botones / scroll / USB	HP		Bueno
			9	Monitor	Pantalla plana 18,0” LCD	COMPAQ	CNC017PKFJ	Bueno
	Rosero Myriam	Asistente 2	10	CPU	2 GB RAM / 216 GB HDD Procesador Intel Core 2 Duo / 32 bits	HP	MXJ91500XP	Bueno
			11	Teclado	Latam. / Alfanumérico / PS2	HP		Bueno
			12	Mouse	Láser / 3 botones / scroll / PS2	HP		Bueno
			13	Monitor	Pantalla plana 17,0” Color	SAMSUNG	PE16H9NQ811125J	Bueno
	Uso general		14	Computador Portátil	8 GB RAM / 698 GB HDD Procesador Intel i7 / 64 bits	HP	2CE20927BG	Bueno

Área	Usuario	Cargo	N.	Activo Fijo	Descripción	Marca	Serie	Estado Físico
	Uso general	(Equipo pertenece a sistemas)	15	Computador Portátil	4 GB RAM / 465 GB HDD Procesador Intel i5 / 64 bits	HP	CNU0432PGX	Bueno
	Uso general		16	CPU	4 GB RAM / 464 GB HDD Procesador Intel i5 / 64 bits	HP	MXL41212G5	Bueno
			17	Monitor	Pantalla plana 18,0” LCD	HP	6CM420283N	Bueno
			18	Mouse	Láser / 3 botones / scroll / USB	HP	FCMHH0CJP6B4LU	Bueno
			19	Teclado	Latam. / Alfanumérico / USB	HP		Bueno
Créditos			20	CPU	4 GB RAM / 465 GB HDD Procesador Intel i5 / 64 bits	HP	MLX41212G1	Bueno
			21	Monitor	Pantalla plana 18,0” LCD	HP	6CM42028F8	Bueno
			22	Mouse	Láser / 3 botones / scroll / USB	HP	67436-001	Bueno
			23	Teclado	Latam. / Alfanumérico / USB	HP	724720-161	Bueno
			24	Impresora	LaserJet M401dw / Monocrom.	HP	VNB3D09226	Bueno
			25	Impresora	Matriz de punto / Monocrom.	EPSON	CDUY239173	Bueno
Presidencia	Lluguín Alicia	Secretaria	26	CPU	2 GB RAM / 232 GB HDD Procesador Intel Core 2 Duo / 32 bits	HP	MXJ91407ZY	Bueno
			27	Mouse	Láser / 3 botones / scroll / PS2	HP	FB7330AN3X020XE	Bueno
			28	Monitor	Pantalla cuadrada 17,0”	HP	3CQ9070Y3G	Bueno
			29	Teclado	Latam. / Alfanumérico / PS2	HP	BC3370GVBWY7VR	Bueno

Área	Usuario	Cargo	N.	Activo Fijo	Descripción	Marca	Serie	Estado Físico
Consejo de administrac.	Lluguín Alicia	Secretaria	30	CPU	4 GB RAM / 464 GB HDD Procesador Intel i7 / 64 bits	HP	MXL4081JCL	Bueno
			31	Mouse	Láser / 3 botones / scroll / USB	HP	FCMHF0A9W55979	Bueno
			32	Monitor	Pantalla plana 18,0” LCD	HP	6CM3462FC0	Bueno
			33	Teclado	Latam. / Alfanumérico / USB	HP	BDMEP0CVB5SS4N	Bueno
			34	Impresora	LaserJet M1319 / Monocrom.	HP	CNJ99C0B05	Bueno
		Auditor	35	CPU	4 GB RAM / 464 GB HDD Procesador Intel i7 / 64 bits	HP	MXL4081JCK	Bueno
			36	Mouse	Láser / 3 botones / scroll / USB	HP	FCMHF0A9W5597K	Bueno
			37	Monitor	Pantalla plana 18,0” LCD	HP	6CM3462CNB	Bueno
			38	Teclado	Latam. / Alfanumérico / USB	HP	BDMEP0CVB5X3Z9	Bueno
			39	Impresora	LaserJet 1018 / Monocrom.	HP		Bueno
Captaciones		Oficial de captaciones	40	CPU	4 GB RAM / 464 GB HDD Procesador Intel i7 / 64 bits	HP	MXL4081K4B	Bueno
			41	Mouse	Láser / 3 botones / scroll / USB	HP	FCHHF0A9W559SL	Bueno
			42	Monitor	Pantalla plana 18,0” LCD	HP	6CM3462CNC	Bueno
			43	Teclado	Latam. / Alfanumérico / USB	HP		
			44	Impresora	LaserJet M1319 / Monocrom.	HP	CNB1M14687	Bueno

Área	Usuario	Cargo	N.	Activo Fijo	Descripción	Marca	Serie	Estado Físico
Créditos		Asistente de Crédito	45	CPU	4 GB RAM / 465 GB HDD Procesador Intel i5 / 64 bits	HP	MXL4081JC6	Bueno
			46	Monitor	Pantalla plana 18,0” LCD	HP	6CM3462CVJ	Bueno
			47	Mouse	Láser / 3 botones / scroll / USB	HP	FCMHF0A9W55994	Bueno
			48	Teclado	Latam. / Alfanumérico / USB	HP	BDMEP0CVB5S01I	Bueno
			49	Impresora	LaserJet M401dw / Monocrom.	HP	CNB9M09613	Bueno
			50	Impresora	Matriz de punto / Monocrom.	EPSON	G8DY494081	Bueno
Auditoría		Auditoría Interna	51	CPU	2 GB RAM / 297 GB HDD Procesador Intel i3 / 32 bits	HP	MXL0382C5X	Bueno
			52	Monitor	Pantalla plana 18,0” LCD	COMPAQ	CNC013Q7C2	Bueno
			53	Mouse	Láser / 3 botones / scroll / USB	HP		Bueno
			54	Teclado	Latam. / Alfanumérico / USB	HP	BBAWE0JGAYY01W	Bueno
			55	Impresora	LaserJet P2015dn / Monocrom.	HP	CNBJM67155	Bueno
	Uso general		56	Copiadora	4 bandejas / WorDcentre 5845	XEROX	152506400	Bueno
Caja	Hernández Marcia Lorena	Jefe caja	57	CPU	2 GB RAM / 298 GB HDD Procesador Intel Core2 Quad / 64 bits	HP	MXJ94603V4	Bueno
			58	Monitor	Pantalla plana 18,0” LCD	COMPAQ	CNT939CKMC	Bueno
			59	Mouse	Láser / 3 botones / scroll / PS2	HP	FB7330A5BXV0SRC	Bueno
			60	Teclado	Latam. / Alfanumérico / PS2	GENIUS	WE2792034360	Bueno

Área	Usuario	Cargo	N.	Activo Fijo	Descripción	Marca	Serie	Estado Físico
			61	Impresora	LaserJet P2055dn / Monocrom.	HP	CNB9N14608	Bueno
			62	Impresora	Matriz de punto / Monocrom.	EPSON	NZBY089167	Bueno
			63	Switch	3com 2106	CDM	AC/9N4Q9F0014495	Bueno
			64	Central Telefónica		Panasonic	4GASS095574	Bueno
Caja 2		Cajera	65	CPU	2 GB RAM / 298 GB HDD Procesador Intel Core2 Quad / 32 bits	HP	MXJ94603TY	Bueno
			66	Monitor	Pantalla plana 18,0” LCD	COMPAQ	CNT939CKLT	Bueno
			67	Mouse	Láser / 3 botones / scroll / USB	HP		Bueno
			68	Teclado	Latam. / Alfanumérico / USB	HP		Bueno
			69	Impresora	Matriz de punto / Monocrom.	EPSON	NZBY095484	Bueno
Caja 3			70	CPU	2 GB RAM / 281 GB HDD Procesador Intel Core2 Quad / 32 bits	HP	MXJ94603V3	Bueno
			71	Monitor	Pantalla plana 18,0” LCD	HP	6CM21314YP	Bueno
			72	Mouse	Láser / 3 botones / scroll / USB	GENIUS	161040605153	Bueno
			73	Teclado	Latam. / Alfanumérico / USB	HP	435302-101	Bueno
			74	Impresora	Matriz de punto / Monocrom.	EPSON	G8DY131825	Bueno
			75	CPU	2 GB RAM / 281 GB HDD Procesador Intel Core2 Quad / 32 bits	HP	MXJ94603V3	Bueno

Área	Usuario	Cargo	N.	Activo Fijo	Descripción	Marca	Serie	Estado Físico
			76	Monitor	Pantalla plana 18,0” LCD	HP	6CM21314YP	Bueno
			77	Mouse	Láser / 3 botones / scroll / USB	GENIUS	161040605153	Bueno
Secretaría general	Ortiz Coronel Vilma Susana	Secretaria General	78	CPU	4 GB RAM / 465 GB HDD Procesador Intel i7 / 64 bits	HP	MXL4081K4H	Bueno
			79	Monitor	Pantalla plana 18,0” LCD		6CM3462F42	Bueno
			80	Mouse	Láser / 3 botones / scroll / USB	HP		Bueno
			81	Teclado	Latam. / Alfanumérico / USB	HP	724718-161	Bueno
			82	Impresora	LaserJet P2050dn / Monocrom.	HP	CNB9021856	Bueno
			83	Escáner	Scanjet 5590	HP	CN8CHT10DW	Bueno
Sistemas	Escobar Parra Vilma Lorena	Admin. de Sistemas	84	CPU	4 GB RAM / 464 GB HDD Procesador Intel i7 / 64 bits	HP	MXL4081JVC	Bueno
			85	CPU	2 GB RAM / 297 GB HDD Procesador Intel i3 / 64 bits	HP	MXL039052L	Bueno
			86	Monitor	Pantalla plana 18,5” LCD	COMPAQ	CNC013Q7B0	Bueno
			87	Monitor	Pantalla plana 18,5” LCD	HP	6CM3462D20	Bueno
			88	Monitor de vigilancia	Pantalla plana 19,0” LCD	HP	CNN7464F04	Bueno
			89	Mouse	Láser / 3 botones / scroll / USB	HP	FCMHF0A9W5S97X	Bueno
			90	Mouse	Láser / 3 botones / scroll / USB	GENIUS	X80369805330	Bueno
			91	Teclado	Latam. / Alfanumérico / USB	HP	BDMEP0CVB5X3Z8	Bueno

Área	Usuario	Cargo	N.	Activo Fijo	Descripción	Marca	Serie	Estado Físico
			92	Teclado	Latam. / Alfanumérico / USB	HP	BBAWE0JVBZ04 MM	Bueno
			93	Impresora	LaserJet P2055dn / Monocrom.	HP	CNB9016584	Bueno
			94	Servidor	Réplica de base de datos SO Linux Cento 6 Procesador Intel Xeon 2.66 Ghz DVD RW Light Scribe 2 HDD externos SCSI 164 GB c/u	HP	2UX81505SL	Bueno
			95	Servidor	Servidor de aplicaciones Procesador Xeon 528 MB en RAM HDD 2 externos ultra SCSI 36,4 GB	HP	F340LK8C1009	Bueno
			96	Servidor	E5620 1P 8GB US Procesador Intel Xeon 2,4 Ghz, 12 MB L3 CACHE, 80W, DDR3-1066, HT, RAID 5, HDD 3 SAS 300 FORM FACTOR RACK LECTOR DVD Light Scribe.	HP	MXQ033037V	Bueno
			97	Servidor	X5690 HPM US INTEL XEON X5690 3,46 Ghz 6 CORE / 12 MB / 130 W DDR 133 CACHE DEVEL , 2 DISCOS DE 1 TERA	HP		Bueno

Área	Usuario	Cargo	N.	Activo Fijo	Descripción	Marca	Serie	Estado Físico
Gerencia	Oña Mendoza César Alfonso	Gerente general	98	Impresora	LaserJet 1320, Monocrom. 2 bandejas	HP	CNHC5D10YM	Bueno
			99	Impresora	LaserJet CP2025, Color 2 bandejas	HP	CNGS204881	Bueno
			100	Máquina de escribir	Eléctrica con visor 0.31A	BROTHER	K1D511213	Bueno
			101	Regulador de voltaje	8 tomas, FVR 1211B	FORZA	09310931314	Bueno
			102	Supresor de picos	6 tomas	ACE		Bueno
			103	Disco duro externo	500 GB/7200 RPM/ APOLLO M100	IMATION		Bueno
			104	Computador Portátil	8GB RAM / 750GB RAM Intel i7 / 64 bits	HP	2CE20927FQ	Bueno
			105	Adaptador computador portátil	Salida 6.5 a 120 W para portátil DV6	HP	WBGTE0BHH105RK	Bueno
			106	Proyector	2700 Lumens/ 1280*800 HDMI/ Lápiz óptico	INFOCUS	BFJM112A1391	Bueno
			107	Computador Portátil	8GB RAM / 1 TB RAM Intel i3 / 64 bits	HP	CND5114805	Bueno
			108	Proyector	S18+	EPSON	V9TK5210354	Bueno

Área	Usuario	Cargo	N.	Activo Fijo	Descripción	Marca	Serie	Estado Físico
			109	Ventilador para computador portátil	5 posiciones / 4 entradas USB 2.0 / silencioso	ERGOS TAND		Bueno
			110	Hub	4 entradas USB / azul	R-LIP		Bueno
Se totalizan 110 artículos en la toma física realizada.								

Fuente: Toma física
Elaborador por: Autor