ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

CARRERA DE CONTABILIDAD Y AUDITORÍA

UDITORÍA INFORMÁTICA A LA COOPERATIVA DE AHORRO Y CRÉDITO "EDUCADORES DE CHIMBORAZO" LTDA. DE LA CIUDAD DE RIOBAMBA, PERÍODO 2018

Trabajo de titulación

Tipo: Proyecto de Investigación

Presentado para optar al grado académico de:

INGENIERO EN CONTABILIDAD Y AUDITORÍA

AUTOR: PAÚL ALEJANDRO MERIZALDE GUAMANZARA

Riobamba – Ecuador

2020

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

CARRERA DE CONTABILIDAD Y AUDITORÍA

AUDITORÍA INFORMÁTICA A LA COOPERATIVA DE AHORRO Y CRÉDITO "EDUCADORES DE CHIMBORAZO" LTDA. DE LA CIUDAD DE RIOBAMBA, PERÍODO 2018

Trabajo de titulación

Tipo: Proyecto de Investigación

Presentado para optar al grado académico de:

INGENIERO EN CONTABILIDAD Y AUDITORÍA

AUTOR: PAÚL ALEJANDRO MERIZALDE GUAMANZARA

DIRECTOR: Ing. Willian Geovanny Yanza Chávez

Riobamba – Ecuador

2020

Yo, Paúl Alejandro Merizalde Guamanzara, declaro que el presente trabajo de titulación es de mi autoría y los resultados del mismo son auténticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este trabajo de titulación; el patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 8 de diciembre de 2020

Paúl Alejandro Merizalde Guamanzara

1715512826

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

CARRERA DE CONTABILIDAD Y AUDITORÍA

El Tribunal del Trabajo de Titulación certifica que: El trabajo de titulación; tipo: Proyecto de Investigación, **AUDITORÍA INFORMÁTICA A LA COOPERATIVA DE AHORRO Y CRÉDITO "EDUCADORES DE CHIMBORAZO" LTDA. DE LA CIUDAD DE RIOBAMBA, PERÍODO 2018**, realizado por el señor: **PAÚL ALEJANDRO MERIZALDE GUAMANZARA**, ha sido minuciosamente revisado por los Miembros del Tribunal del trabajo de titulación, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

	FIRMA	FECHA
Ing. Luis Sanandres Alvares **PRESIDENTE DEL TRIBUNAL**	LUIS GERMAN SANANDRES ALVAREZ Firmado digitalmente por LUIS GERMAN SANANDRES ALVAREZ Fecha: 2020.12.20 23:55:15 -05'00'	2020-12-08
Ing. Willian Geovanny Yanza Chávez **DIRECTOR DE TRABAJO DE TITULACIÓN**	WILLIAN GEOVANNY YANZA CHAVEZ WILLIAN GEOVANNY YANZA CHAVEZ c=EC, l=RIOBAMBA, serialNumber=0602356214, cn=WILLIAN GEOVANNY YANZA CHAVEZ	2020-12-08
Ing. Hítalo Bolívar Veloz Segovia **MIEMBRO DEL TRIBUNAL**	HITALO BOLIVAR VELOZ SEGOVIA Firmado digitalmente por HITALO BOLIVAR VELOZ SEGOVIA Fecha: 2020.12.21 09:50:53 -05'00'	2020-12-08

DEDICATORIA

A mis queridos padres Jaime y Albita, que han estado conmigo en cada paso apoyándome y alentándome a seguir avanzando y cumpliendo mis metas, a mis hermanas y hermanos por ayudarme y alentarme en mis estudios, a toda mi familia que con su apoyo me ayudo a lograr este objetivo y por ultimo a todas las personas que me guiaron y me enseñaron a ser el hombre que soy.

PAÚL

AGRADECIMIENTO

A la vida por dejarme alcanzar mis metas, a mis padres Albita y Jaime por ayudarme y su dedicación constante para lograr mis metas, a Susanita por orientarme para lograr este objetivo, a mis hermanas y hermanos, a mi familia, a todos mis profesores de la Escuela de Contabilidad y Auditoría que me brindaron los conocimientos necesarios y me enseñaron como actuar en el mundo laboral, y además a todos mis amigas y amigos que conocí en el transcurso de mi carrera

PAÚL

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

Se realizó una Auditoría Informática a la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda.(COAC), de la Ciudad de Riobamba, período 2018, mediante la información emitida por la Institución facilitadora, con el fin de obtener el nivel de confiabilidad y el grado de eficiencia eficacia de los recursos tecnológicos disponibles en la organización, revisando el cumplimiento de las normas básicas de Control Interno. A través de la relación laboral se recopiló la información necesaria mediante de la utilización de cuestionarios de control interno, la observación y la entrevista a los colaboradores de la organización, se aplicó el sistema de control interno COSO II, logrando obtener los hallazgos donde se encuentran las recomendaciones con soluciones descritas y basadas en la Norma de Calidad ISO 27002, mitigando el riesgo de control. En la presentación de los resultados se encuentra principalmente la falta de procedimientos ante interrupciones del sistema, la falta de un contrato de seguro de activos, la falta de comunicación de las Políticas de Seguridad y la falta de recursos disponibles para el mejoramiento de los equipos, lo que provoca desactualización y perdidas económicas. Como recomendación a la organización se establece realizar un contrato con una firma auditora autorizada, la que le permita entregarle una evaluación profunda del estado de la COAC en los Sistemas Informáticos y promueva su desarrollo y mejore la toma de decisiones gerenciales

Palabras Clave: <AUDITORÍA> <SEGURIDAD INFORMÁTICA> <SISTEMA DE CONTROL INTERNO> <COSO II> <NORMA ISO 27002> <SEGURIDAD FÍSICA> <SEGURIDAD LÓGICA> <TECNOLOGÍAS DE LA INFORMACIÓN (TICS)>

ABSTRACT

A computer audit was carried out at the Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda.(COAC), located in Riobamba city, term 2018, through the information issued by the facilitating institution, in order to obtain the level of reliability and the degree of efficiency of the technological resources available in the organization, reviewing the compliance with the basic rules of Internal Control. Through the labor relationship the necessary information was collected through the use of internal control questionnaires, the observation and interview of the organization's employees; the control system applied the internal control system COSO II, obtaining the findings where the recommendations are found with solutions described and based on the Quality Standard ISO 27002, reducing the risk of control. In the presentation of results it is evident the lack of processes due to system interruptions, lack of an asset insurance contract, lack of communication of security policies and the lack of resources for the improvement of equipment, which causes out-of-date and economic losses. As a recommendation to the organization, it is required to make a contract with an authorized audit firm, which allows to provide an in-depth evaluation of the situation of the COAC within the Information Systems to promote the development and improve the management of the company.

Keywords: <AUDITING> <COMPUTER SECURITY> <INTERNAL CONTROL SYSTEM > <COSO II> <ISO 27002> <PHYSICAL SAFETY> <LOGICAL SECURITY> <INFORMATION TECHNOLOGIES (TICS)>

INTRODUCCIÓN

En la actualidad la Tecnología avanza a pasos agigantados, convirtiéndose en necesario para la realización de las actividades laborales y cotidianas de las personas en todo el globo, permitiendo además crear mayor cantidad de ganancias a menores costos.

Con la globalización la informática ha permitido mejorar e influenciar el sector financiero, dotándolo de herramientas las cuales le permiten relacionarse y satisfacer las necesidades de los socios (clientes) facilitando la interacción y los servicios a través de la red, logrando inclusive la banca móvil, las transacciones electrónicas, depósitos y retiros entre entidades de la banca y cooperativa.

La realización sistemática de una Auditoria aplicando el sistema de control COSO II y la Normas ISO 27002 mejora el uso de los recursos Tecnológicos, además encuentra de manera rápida el nivel de confianza, el grado de economía, eficiencia, eficacia, logrando calcular el nivel de efectividad de las organizaciones auditadas.

Por lo anteriormente descrito se realizó una Auditoría entregando un informe de auditoría a la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo", analizando el uso de los recursos, el cumplimiento de objetivos en el periodo 2018, ubicada en la provincia de Chimborazo, cantón de Riobamba, y plantea lo siguiente.

En el Capítulo I se encuentra descrito el problema de investigación, los objetivos y la justificación del trabajo de investigación.

En el Capítulo II se detalla el Marco Teórico Referencial, cuyo contenido se encuentra el material bibliográfico, conceptos necesarios para la Auditoria Informática, las fases y procedimientos para su ejecución y posterior informe.

En el Capítulo III se describe el Marco Metodológico, encontrándose la idea a defender, la población, los métodos, técnicas y herramientas de investigación

En el Capítulo IV encontramos el Marco Propositivo, en el cual se encuentra la Planificación, la Ejecución y el Informe de Auditoria donde se encuentran los hallazgos y las recomendaciones necesarias para mejorar la toma de decisiones gerenciales

CAPÍTULO I

1. MARCO TEÓRICO REFERNCIAL

1.1. Planteamiento del problema

A nivel mundial, la auditoría informática se realiza con carácter objetivo, crítico, sistemático y selectivo con el fin de evaluar la eficacia y eficiencia del uso adecuado de los recursos informáticos, de la gestión informática y si han brindado el soporte adecuado a los objetivos y metas del negocio.

La mayoría de las empresas trabajan online sin tener un mínimo de conocimientos sobre informática. Es cierto que alguien con experiencia a nivel usuario puede acceder a un operador, pero si se trata de cuestiones técnicas es diferente.

Las empresas tienen necesidades cada día más complejas y eso implica utilizar el personal disponible el que en ocasiones no está capacitado. Es ahí donde empiezan a producirse problemas informáticos en la empresa, que se han ido acumulando con el tiempo.

Los más importantes:

- Riesgos para la seguridad en su página web para las compras online.
- Manejo incorrecto de los ordenadores de la empresa (usos indebidos, almacenamiento de archivos ajenos al negocio, etc.)
- Ausencia de medidas de seguridad preventivas en el cuidado del software, como por ejemplo un sistema de backups online.
- Falta de una política de contingencia ante problemas informáticos como virus, etc.
- Escasa velocidad y falta de optimización en las redes informáticas de la empresa.

Ante un problema informático generalizado, lo mejor que puede hacer una empresa es adoptar una actitud proactiva y realizar un giro a la empresa. Invertir en seguridad informática significa clientes satisfechos, reducción al mínimo de peligros y menos gastos en hardware por razones de falta de mantenimiento.

En el caso Latinoamericano se evidencia el uso de grandes sistemas informáticos financieros que

sin un control de su actividad, estos colapsarían y provocarían grandes pérdidas para quienes dependen de ellos, proyectando una mala imagen de las mismas.

Las Auditorías Informáticas deben hacerse de forma periódica de tal forma que detecten las fallas o falencias y ayuden a corregirlas. Además hay que citar que el avance de la tecnología crece a pasos agigantados, creándose e inventándose día a día mejores y más sofisticados equipos que permiten optimizar la función de los Sistemas Informáticos Financieros.

En la auditoría informática se investigan todos y cada uno de los aspectos importantes relacionados con los dispositivos informáticos de la empresa para que funcionen óptimamente: velocidad, seguridad, escalabilidad, prevención y mantenimiento; con una política general de informática para conseguir los siguientes objetivos:

- Optimizar los recursos disponibles para que funcionen con un buen rendimiento.
- Analizar las posibilidades futuras de acuerdo con la estrategia de la empresa.
- Establecer una política de mantenimiento informático preventivo para el aprovechamiento de los equipos.
- Transmitir a la plantilla la información necesaria para el manejo de los dispositivos informáticos sin ocasionar problemas.
- Establecimiento de una política de seguridad online. Página web, redes sociales, correos electrónicos, servidor, etc.
- Crear unas líneas de actuación en caso de contingencias informáticas para que todo se desarrolle de acuerdo con lo previsto.
- Estudiar la composición de la red informática de la empresa y comprobar que es lo suficiente óptima.

En definitiva, el objetivo es advertir qué se está haciendo incorrecto y corregirlo, qué se está haciendo bien, pero se puede hacer mejor y cuáles van a ser los protocolos de actuación (mantenimiento correctivo) en el caso de problemas para que esto no afecte directamente a la productividad de la empresa.

Específicamente en Ecuador, en la Ciudad de Riobamba, hace aproximadamente 55 años, viendo la necesidad que tenían los profesores, en la Oficina de la Inspección Escolar, nace la idea de formar una Cooperativa de Ahorro y Crédito, la cual sería para su beneficio y también para la ciudad de Riobamba.

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.

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.

La Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" de la ciudad de Riobamba dispone de los equipos necesarios para cumplir con excelencia la atención a sus afiliados, pero existe ordenadores que poseen programas innecesarios, es por ello que se ve la necesidad de realizar una auditoria informática para determinar las falencias que puede tener cada ordenador en los diferentes departamentos de esta cooperativa y de esta manera agilitar la eficiencia del sistema y atención a los clientes.

Después de realizar un análisis a la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo, se encontró falencias las cuales se puede citar:

- Manejo inadecuado de los equipos informáticos, lo que provoca que los mismos se deterioren con facilidad y tengan que ser desechados.
- La Velocidad de navegación Web es lenta y esto dificulta el buen funcionamiento correcto de la COAC.
- Inseguridad de la información que se almacena en los equipos informáticos esto provoca salida de información de uso exclusivo de la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda.
- Carencia de un plan de contingencia para prevenir riesgos en la información lo cual dificulta el accionar de los funcionarios de la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda., ante cualquier eventualidad suscitada con el sistema informático – operativo

Con lo expuesto anteriormente se enfocara que el problema se relaciona a falta de una auditoria a los sistemas informáticos que servirá como una herramienta para la toma de decisiones de parte de la Gerencia.

1.2. Formulación del problema

¿Cómo la Auditoría Informática a la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda., de la Ciudad de Riobamba. Período 2018, mejorara la eficiencia y la eficacia dentro de la Institución y facilitara el desenvolvimiento del personal?

1.3. Sistematización del problema

Tema: Auditoría Informática a la COAC
Empresa: Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda.
Provincia: Chimborazo
Cantón: Riobamba
Campo: Administración
Área: Auditoría
Aspecto: Eficiencia de los Sistemas y Servicios e información
Dirección: Veloz 22-11 y Espejo

1.4. Objetivos

Objetivo General

Realizar una Auditoría Informática a la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda., de la Ciudad de Riobamba, período 2018, mediante la información emitida por la Institución facilitadora, y emitir el informe de Auditoría el cual servirá de herramienta para la toma de decisiones Gerenciales.

Objetivos Específicos

- Elaborar el marco teórico con la utilización de fuentes bibliográficas actualizada y especializada, de tal forma que sirvan para sustentar la presente investigación.
- Efectuar la recopilación de la información necesaria y la aplicación del COSO II (E.R.M), a través de las fuentes de primarias y secundarias, y con esto recabar los datos necesarios para la Investigación.
- Ejecutar la Auditoría Informática al Área de Sistemas de la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda., de la Ciudad de Riobamba, periodo 2018, mediante la información emitida por la Institución facilitadora, y con eso presentar un informe de Auditoría el cual servirá de herramienta para la toma de decisiones Gerenciales.

1.5. Justificación

Justificación Teórica

A fin de realizar una justificación teórica se basara en la aplicación del COSO II (E.R.M) el que proporciona el cumplimiento de todos los objetivos previstos, además se busca aprovechar todo el referencial teórico sobre la Auditoría, específicamente la Auditoría Informática al Área de Sistemas de tal forma que sirva de herramienta de toma de Decisión Gerencial.

Justificación Metodológica

La presente investigación se justificara de forma metodológica a través de la aplicación de la recolección de la información necesaria para un correcto desarrollo, las técnicas que se utilizaran son la entrevista y la encuesta ya que se tiene el apoyo por parte de la Institución facilitadora, a fin de recabar información relevante, pertinente y consistente para la elaboración de la Auditoría Informática, de tal manera que sus resultados sean los más objetivos y reales posibles.
Dicha información requerida se obtendrá de manera directa de la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda. Se utilizarán técnicas de investigación de fuente primaria como son la entrevista la que se dirigirá al personal en Sistemas para que facilite la identificación de los posibles hallazgos y es una fuente de recolección usada con más frecuencia.

Justificación Académica

Se pondrá en práctica todos los conocimientos adquiridos durante el trascurso de la Carrera para lograr dar una Justificación Académica, en la realización de la Auditoria Informática; paralelamente nos permite adquirir nuevos conocimientos relacionados, siendo éste un requisito importante para la culminación y obtención del Título de Grado de Ingeniería en Contabilidad y Auditoría.

Justificación Práctica

Se elaborara la Auditoria Informática al Área de Sistemas de la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda., para poder cumplir con la Justificación Practica entre otros aspectos incluirá: el análisis del sistema Informático utilizado dentro de la empresa, de tal forma que permitirá mejorar la eficiencia y eficacia en la utilización de los Sistemas de Información, así como el correcto cumplimiento de la normativa legal que le es aplicable a esta organización.

1.6. Marco de referencias

1.6.1. *Antecedentes de investigación*

El 26 de junio de 1964 se creó la Cooperativa de Ahorro y Crédito Educadores de Chimborazo, CACECH; es una Institución financiera Cooperativista de carácter de Gremio exclusivo, con más de 4000 socios quienes pertenecen al Magisterio de la provincia de Chimborazo, realizan aportaciones mensuales que les permite gozar de servicios adicionales como descuentos, seguro de vida, entre otros con empresas con la que la Cooperativa tiene convenios.

Entre los productos financieros que ofrece la COAC se encuentra: Libretas de Libre Ahorro – Libre Retiro; Libreta de Ahorro Cautivo y Fondos de Reserva; Inversiones a plazo fijo con el mejor interés en el mercado; permitiendo a los socios de la Cooperativa, el acceso a créditos como: Anticipo de Sueldo, Emergencia, Ordinario, y CREDIFLASH, conforme a su necesidad y capacidad de pago, con un monto máximo de 20.000 dólares.

Referente a la Dirección esta entidad financiera se encuentra ubicada en el centro histórico la ciudad de Riobamba, capital de la provincia de Chimborazo, en las calles Veloz y Espejo; cuyas instalaciones se encuentran en un edificio de su propiedad, el horario de atención es de Lunes a Viernes de 09:00 a 16:00 sin cerrar a medio día, y Sábados desde las 08:00 a 13:00.

La Cooperativa realiza agasajos a sus socios como entrega de regalos en fechas importantes y además sortea dos automóviles 0 KM en el transcurso del año, el primero en el mes de Julio y el segundo en Diciembre, además en el mes de Diciembre entrega a los socios con mayores movimientos en la cuenta, regalos especiales y el aguinaldo navideño.

Como otro servicio que cuenta la institución es la tarjeta de débito Visa Electrón CACECH, con esta tarjeta se puede realizar pagos de los fondos disponibles en la cuenta, a través de la tarjeta se accede al sueldo que se deposita de manera mensual en cada una de las cuentas por el Sistema de Pagos Interbancarios del Banco Central, el cual es la manera más rápida dentro del sector financiero.

1.7. Marco teórico

1.7.1. *Auditoría*

La Auditoría para su comprensión manifiesta "Auditoría es la acumulación y evaluación de evidencia basada en información para determinar y reportar sobre el grado de correspondencia entre la información y los criterios establecidos. La auditoría debe realizarla una persona independiente y competente". (Arens, A., 2007, p. 4)

Además otro autor dice:

> *La Auditoría como el examen de la información por una tercera persona distinta de quien la preparó y del usuario, con la intención de establecer su veracidad; y el dar a conocer los resultados de este examen, con la finalidad de aumentar la utilidad de tal información para el usuario.* (Porter, L., 1983, p. 46)

Con lo anterior según los Autores se dice que la Auditoría es una tarea que se encarga en recopilar información del procedimiento en cualquier tipo de empresa para poder medir su nivel de cumplimiento.

1.7.2. *Importancia de la Auditoria*

"Proporciona información pertinente y oportuna sobre los problemas que suscitan en la entidad a fin de solucionar y mejorar con ello su funcionamiento, eficiencia y eficacia" (Arens, A., 2007, p. 6). Por otro lado define: "La razón detrás de esto es que el éxito percibido de cualquier organización generalmente se mide por la capacidad del negocio para definir claramente y alcanzar sus objetivos" (Ghafran., 2017, p. 9)

El término de Importancia de la Auditoria, permite el éxito sobre los problemas y busca las soluciones y mide la capacidad del negocio para alcanzar sus objetivos

1.7.3. *Informática*

La Informática es una "Ciencia del tratamiento sistemático y eficaz, realizado especialmente mediante máquinas automáticas, de la información contempladas como vehículo de saber humano, y de la comunicación de los ámbitos técnico, económico y social". (Echenique J., 2009, p. 3)

Con lo anterior dicho manifiesta:

> *Una disciplina emergente-integradora que surge producto de la aplicación-interacción sinérgica de varias ciencias, como la computación, la electrónica, la cibernética, las telecomunicaciones, la matemática, la lógica, la lingüística, la ingeniería, la inteligencia artificial, la robótica, la biología, la psicología, las ciencias de la información, cognitivas, organizacionales, entre otras, al estudio y desarrollo de los productos, servicios, sistemas e infraestructuras de la nueva sociedad de la información.* (Cañedo, R., 2005, p. 8)

1.7.4. ***Riesgos de Auditoría***

Según Objetivo y Principios Generales que Gobiernan una Auditoria de Estados Financieros "Cuando un auditor independiente emite una opinión acerca de la razonabilidad de los estados financieros de una entidad, éste siempre se enfrentará a la posibilidad de que su opinión sea inapropiada (NIA 200, p. 6)

1.7.4.1. *Tipos de Riesgos*

Los Tipos de Riesgo son:

1) *Riesgo Inherente*

   Es la posibilidad de un error material, en una afirmación antes de examinar el control interno de los clientes. Los factores que influyen en él, son la naturaleza del cliente y de su industria o la de una cuenta en particular de los estados financieros.)

2) *Riesgo de Control*

   Es el del cual el control interno no informa oportunamente un error material. Se basa enteramente en la eficacia de dicho control interno.

   Para evaluar este tipo de riesgo, los auditores tienen en cuenta los controles del cliente concentrándose en los que afectan a la confiabilidad de los informes financieros. Los controles bien diseñados que funcionan eficientemente aumentan la confiabilidad de los datos contables.

3) *Riesgo de Detección*

Es el de que los auditores no descubran los errores al aplicar sus procedimientos. En otras palabras, es la posibilidad de que los procedimientos solo lleven a concluir que no existe un error material en una cuenta o afirmación, cuando en realidad si existe. El riesgo se limita efectuando pruebas sustantivas. (Whittington P., 2005, pp.119 120)

1.7.5. *Auditoría Informática*

La Auditoría nos dice:

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. (Muñoz, C., 2002, p. 19)

Nos indica que la Auditoría Informática es una revisión que se lo realiza a los sistemas computacionales integrados por Software y Hardware, también de las instalaciones, mobiliario y otros componentes para su correcto funcionamiento.

1.7.6. *Tipos de Auditoría de Sistemas Computacionales*

- Auditoría Informática: Según, dice:
  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 que lo integran. (Muñoz C, 2002, p. 19)
- Auditoria con la Computadora: Se la desarrolla a través de la computadora y varios programas, que permite evaluar las actividades revisadas, con forme a las necesidades del Auditor.
- Auditoria a la Gestión Informática dice:

  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. Su propósito es dictaminar sobre la adecuada gestión administrativa de los sistemas computacionales de

una empresa y del propio centro informático. (Pinilla J., 1994, p. 4).

- Auditoria de la Seguridad de los Sistemas Computacionales: Permite la evaluación de las actividades y las acciones que permitan prevenir y corregir para salvaguardar la seguridad de los equipos de cómputo, la Base de Datos, entre otros.
- Auditoría ISO-9000 a los Sistemas Computacionales manifiesta:
  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", indica que esta Auditoría permite revisar de forma exhaustiva, sistemática y especializada que lo realizan los Auditores especializados y certificados en las normas y procedimientos ISO-9000, donde se aplicaran los lineamientos y los procedimientos establecidos por la asociación. (Muñoz C., 2002, p. 28).

1.7.7. *COSO II (E.R.M.)*

El COSO II es un:

Proceso, efectuado por la junta de directores de una entidad, por la administración y por otro personal, aplicado en el establecimiento de la estrategia y a través del emprendimiento, diseñado para identificar los eventos potenciales que puedan afectar la entidad, y para administrar los riesgos que se encuentran dentro de su apetito por el riesgo, a fin de proveer seguridad razonable en relación con el logro del objetivo de la entidad. (Estupiñan, R., 2015, p. 119).

1.7.7.1. *Beneficios*

Los Beneficios son:

El E.R.M puede realizar una enorme contribución ayudando a la organización a gestionar los riesgos para poder alcanzar sus objetivos.

Los beneficios incluyen:

- *Mayor posibilidad de alcanzar los objetivos.*
- *Consolidado de reportes de riesgos a analizar por la Junta Directiva o Consejo de Administración.*
- *Incrementa el entendimiento de riesgos claves y sus más amplias implicaciones.*

- *Identifica y comparte riesgos alrededor del negocio.*
- *Crea mayor enfoque de la gerencia en asuntos que realmente importan.*
- *Menos sorpresas y crisis.*
- *Mayor enfoque interno en hacer lo correcto en la forma correcta.*
- *Incrementa la posibilidad de que cambios en iniciativas puedan ser logrados.*
- *Capacidad de tomar mayor riesgo por mayores recompensas, y*
- *Más información sobre riesgos tomados y decisiones realizadas* (Estupiñan, R., 2015, p. 134)

1.7.7.2. *Componentes*

a) El Entorno de control:

> *El entorno de control es: El fundamento de todos los otros componentes del E.R.M., creando disciplina y organizando adecuadamente la estructura empresarial, determinando las estrategias y los objetivos, como también estructurando las actividades del negocio e identificando, valorando y actuando sobre los riesgos*. (Estupiñan, R., 2015, p. 68).

b) Definición de Objetivos

La definición de objetivos establece:

> *Dentro del contexto de la misión o visión, se establecen objetivos estratégicos, selecciona estrategias y establece objetivos relacionados, alineados y vinculados con la estrategia, así como los relacionados con las operaciones que aportan efectividad y eficiencia de las actividades operativas, ayudando a la efectividad en la presentación de reportes o informes internos y externos (financiera y no financiera), como la de cumplir con las leyes y regulaciones aplicables y de sus procedimientos internos determinados* (Estupiñan, R., 2015, p.68)

c) Identificación de Eventos

La Identificación de Eventos se da:

> *Los acontecimientos que se dan de manera interna y externa de la organización y que por ende afectan a los objetivos de la Entidad deben ser identificados, diferenciando entre los riesgos (eventos con impacto negativo) y las oportunidades (eventos con impacto positivo). Las oportunidades pueden revertir hacia la estrategia de la dirección o los procesos para fijar objetivos*. (Estupiñan, R., 2015, p. 70)

d) Valoración de Riesgos

La Valoración de Riesgos permite:

A una entidad considerar como los eventos potenciales pueden afectar el logro de los objetivos. La gerencia valora los eventos bajo las perspectivas de probabilidad (posibilidad de que ocurra un evento) e impacto (su efecto debido a su ocurrencia), con base en datos pasados internos (pueden considerarse de carácter subjetivo) y externos (son más objetivos). (Estupiñan, R., 2015, p. 72)

e) Respuesta al Riesgo

Nos dice:

Una vez que la gerencia ha evaluado los riesgos importantes debería determinar cómo hacerles frente, ya sea evitando, reduciendo, compartiendo y/o aceptando el riesgo. Al considerar su respuesta la gerencia evalúa su efecto y la probabilidad de impacto del riesgo, así como los costos y beneficios involucrados, seleccionando aquella que ubique el riesgo residual dentro de las tolerancias al riesgo establecidas por la organización. (Estupiñan, R., 2015, p.78)

f) Actividades de Control

Son:

Son aquellas que realizan la gerencia y demás personal de la organización para cumplir diariamente con las actividades asignadas. Estas actividades están expresadas en las políticas, sistemas y procedimientos.

Ejemplos de estas actividades son la aprobación, la autorización, la verificación, la conciliación, la inspección, la revisión de indicadores de rendimiento, la salvaguarda de los recursos, la segregación de funciones, la supervisión y entrenamiento adecuados. (Estupiñan, R., 2015, p.32)

g) Información y Comunicación

Los Sistemas de Información y Comunicación son "Un medio para incrementar la productividad y competitividad. Ciertos hallazgos sugieren que la integración de la estrategia, la estructura organizacional y la tecnología de información es un concepto clave para el nuevo siglo". (Estupiñan, R., 2015, p. 34)

h) Monitoreo

El Monitoreo ocurre en el:

Curso normal de las operaciones, e incluye actividades de supervisión y dirección o administración permanente y otras actividades que son tomadas para llevar a cabo las obligaciones de cada empleado y obtener el mejor sistema de control interno de la organización. (Estupiñan, R., 2015, p. 40)

1.7.8. *ISO 27001 seguridad de la información*

La Organización Internacional de Estandarización (ISO), a través de las normas recogidas en ISO / IEC 27000, establece una implementación efectiva de la seguridad de la información empresarial desarrolladas en las normas ISO 27001 / ISO 27002.

Los requisitos de la Norma ISO 27001 norma nos aportan un Sistema de Gestión de la Seguridad de la Información (SGSI), consistente en medidas orientadas a proteger la información, indistintamente del formato de la misma, contra cualquier amenaza, de forma que garanticemos en todo momento la continuidad de las actividades de la empresa.

Los Objetivos del SGSI son preservar la:

- Confidencialidad
- Integridad
- Disponibilidad de la Información

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización.

1.7.8.1. *Función de la ISO 27001*

Es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

Figura 1-2: Estructura de ISO 27001
Fuente: 2020, https://advisera.com/27001academy/es/que-es-iso-27001/

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.
Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI).
Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, anti-virus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.

1.7.8.2. *Importancia de la ISO 27001*

Hay 4 ventajas comerciales esenciales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información:
Cumplir con los requerimientos legales – cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La buena noticia es que la mayoría de ellos se pueden resolver implementando ISO 27001 ya que esta norma le proporciona una metodología perfecta para cumplir con todos ellos.

Obtener una ventaja comercial – si su empresa obtiene la certificación y sus competidores no, es posible que usted obtenga una ventaja sobre ellos ante los ojos de los clientes a los que les interesa mantener en forma segura su información.

Menores costos – la filosofía principal de ISO 27001 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o pequeño, cuesta dinero; por lo tanto, evitándolos su empresa va a ahorrar mucho dinero. Y lo mejor de todo es que la inversión en ISO 27001 es mucho menor que el ahorro que obtendrá.

Una mejor organización – en general, las empresas de rápido crecimiento no tienen tiempo para hacer una pausa y definir sus procesos y procedimientos; como consecuencia, muchas veces los empleados no saben qué hay que hacer, cuándo y quién debe hacerlo.

La implementación de ISO 27001 ayuda a resolver este tipo de situaciones ya que alienta a las empresas a escribir sus principales procesos (incluso los que no están relacionados con la seguridad), lo que les permite reducir el tiempo perdido de sus empleados.

1.7.8.3. *Contenido de la ISO 27001*

Sección 0 Introducción explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión.

Sección 1 Alcance: explica que esta norma es aplicable a cualquier tipo de organización.

Sección 2 Referencias normativas: hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.

Sección 3 Términos y definiciones: de nuevo, hace referencia a la norma ISO/IEC 27000.

Sección 4 Contexto de la organización: esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI.

Sección 5 Liderazgo: esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.

Sección 6 Planificación: esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.

Sección 7 Apoyo: esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

Sección 8 Funcionamiento: esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.

Sección 9 Evaluación del desempeño: esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.

Sección 10 Mejora: esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

Anexo A este anexo proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones (secciones A.5 a A.18).

Obtención de la Certificación

Existen dos tipos de certificados ISO 27001: **(a) para las organizaciones y (b) para las personas**. Las organizaciones pueden obtener la certificación para demostrar que cumplen con

todos los puntos obligatorios de la norma; las personas pueden hacer el curso y aprobar el examen para obtener el certificado.
Para obtener la certificación como organización, se debe implementar la norma tal como se explicó en las secciones anteriores y luego se debe aprobar la auditoría que realiza la entidad de certificación.

1.7.8.4. *Pasos para la Obtención de la ISO 27001*

1° Paso de la auditoría (revisión de documentación): los auditores revisarán toda la documentación.

2° Paso de la auditoría (auditoría principal): los auditores realizarán la auditoría in situ para comprobar si todas las actividades de una empresa cumplen con ISO 27001 y con la documentación del SGSI.

Visitas de supervisión: después de que se emitió el certificado, y durante su vigencia de 3 años, los auditores verificarán si la empresa mantiene su SGSI.

1.7.9. ***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
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,

1.7.9.1. *Dominios de la norma ISO 27002*

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.

1.7.10. *Normas de control interno de la contraloría general del estado*

1.7.10.1. *Norma 410 tecnologías de la información*

Organización informática **las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional, La Unidad de Tecnología de Información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica**	**Segregación de funciones** **Se debe realizar dentro de la Unidad de Tecnología de Información la supervisión de roles y funciones del personal dentro de cada una de las áreas, para gestionar un adecuado rendimiento y evaluar las posibilidades de reubicación e incorporación de nuevo personal.**
Plan informático estratégico de tecnología **La Unidad de Tecnología de Información elaborará planes operativos de tecnología de la información alineados con el plan estratégico informático y los objetivos estratégicos de la institución, dichos planes asegurarán que se asignen los recursos apropiados de la función de servicios de tecnología de información a base de lo establecido en su plan estratégico**	Políticas y procedimientos La Unidad de Tecnología de Información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización
Modelo de información organizacional **La Unidad de Tecnología de Información definirá el modelo de información de la organización a fin de que se facilite la creación, uso y compartición de la misma; y se garantice su disponibilidad, integridad, exactitud y seguridad sobre la base de la definición e implantación de los procesos y procedimientos correspondientes**	Administración de proyectos tecnológicos La Unidad de Tecnología de Información definirá mecanismos que faciliten la administración de todos los proyectos informáticos que ejecuten las diferentes áreas que conformen dicha unidad
Desarrollo y adquisición de software aplicativo **La Unidad de Tecnología de Información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos**	Adquisiciones de infraestructura tecnológica La Unidad de Tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la organización
Mantenimiento y control de la infraestructura tecnológica **La Unidad de Tecnología de Información de cada organización definirá y regulará los**	Seguridad de tecnología de información La Unidad de Tecnología de Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los

procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades	medios físicos y la información que se procesa mediante sistemas informáticos
Plan de contingencias **La Unidad de Tecnología de Información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.**	Administración de soporte de tecnología de información La Unidad de Tecnología de Información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos
Monitoreo y evaluación de los procesos y servicios **Definirá sobre la base de las operaciones de la entidad, indicadores de desempeño y métricas del proceso para monitorear la gestión y tomar los correctivos que se requieran.**	Sitio web, servicios de internet e intranet Es responsabilidad de la Unidad de Tecnología de Información elaborar las normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio web de la entidad, a base de las disposiciones legales y normativas y los requerimientos de los usuarios externos e internos
Capacitación informática **Las necesidades de capacitación serán identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constarán en un plan de capacitación informático, formulado conjuntamente con la Unidad de Talento Humano**	Comité informático Se considerarán los siguientes aspectos: El tamaño de la entidad La definición clara de los objetivos que persigue la creación de un Comité de Informática La conformación y funciones del comité
Firmas electrónicas **Las entidades, organismos y dependencias del sector público, así como las personas jurídicas que actúen en virtud de una potestad estatal, ajustarán sus procedimientos y operaciones e incorporarán los medios técnicos necesarios, para permitir el uso de la firma electrónica de conformidad con la Ley de Comercio Electrónico**	

Figura 2-2: Normas de control interno de la Contraloría general del Estado
Fuente: Normas de control interno de la contraloría General del estado
Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

1.7.11. *Control interno y control interno informático*

1.7.11.1. *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, R., 2002, p. 106)

1.7.11.2. *Características del control*

Las Características del control son:

> *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, R., 2002, p. 101)

1.7.12. *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

Figura 3-2: Control Interno en el Área Informática

Fuente: Carlos Muñoz Razo, 2002

Recuperado de: https://studylib.es/doc/118940/control-interno-informatico, 2020

1.7.13. *Aspecto técnico*

1.7.13.1. *Software*

Nos dice:

> *Son instrucciones (programas de computadora) que cuando ejecutado proporcionan características, función y rendimiento deseados; estructuras de datos que permiten a los programas manipular adecuadamente información, y información descriptiva tanto en papel como en formularios virtuales que describen el funcionamiento y uso de los programas.* (Pressman, R., 2015, p. 4)

1.7.13.2. *Hardware*

Según, el hardware es:

> *En computación e informática, se conoce como hardware (unión de los vocablos del inglés hard, rígido, y ware, producto, mercancía) al total de los elementos materiales, tangibles, que forman al sistema informático de una computadora u ordenador dentro de la organización.* (Raffino, E., 2020, p. 35)

1.8. Marco conceptual

Auditoría Informática: Es un proceso formal ejecutado por los especialistas del área de auditoría y de informática, el cual se orienta a la verificación y aseguramiento de que las políticas y procedimientos establecidos para el manejo y uso adecuado de la TI en la organización se lleven a cabo de una manera oportuna y eficiente.

Metodología: Es un conjunto de etapas formalmente estructuradas, de manera que brinden a los interesados los siguientes parámetros de acción en el desarrollo de sus proyectos: plan general y detallado, tareas y acciones, tiempos, aseguramiento de la calidad, involucrados, etapas, revisiones de avance, responsables, recursos requeridos, etc.

Controles Correctivos: Son aquellos que corrigen errores, omisiones o actos maliciosos una vez detectados (Verificación de las fechas de las facturas)

Controles de Detección: Son aquellos que detectan que se ha producido un error, omisión o acto malicioso e informan de su aparición (pe. Impresión del registro histórico (log))

Controles Generales: Son controles interdependientes válidos para todas las áreas de la organización.

Controles Preventivos: Son aquellos controles diseñados para evitar que se produzca un error, omisión o acto malicioso. (Software de control de acceso)

1.9. Interrogantes de estudio

1.9.1. *Idea a Defender*

La realización de la Auditoria Informática a la Cooperativa de Ahorro y Crédito “Educadores de Chimborazo” Ltda., de la Ciudad de Riobamba, periodo 2018, promoverá el mejoramiento de la eficiencia, eficacia y economía de la empresa en relación a su recurso informático.

CAPÍTULO II

2. MARCO METODOLÓGICO

2.1. Enfoque de investigación

2.1.1. *Cualitativa*

Nos dice:

> *Profundiza 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*. (Bonilla, E., 2005, p.60)

Por otro lado), se refiere:

> *Se nutre epistemológicamente de la hermenéutica, la fenomenología y el interaccionismo simbólico. El pensamiento hermenéutico parte del supuesto que los actores sociales no son meros objetos de estudio como si fuesen cosas, sino que también significan, hablan, son reflexivos. También pueden ser observados como subjetividades que toman decisiones y tienen capacidad de reflexionar sobre su situación, lo que los configura como seres libres y autónomos ante la simple voluntad de manipulación y de dominación.* (Monje, C., 2011, p.3)

Según los autores nos dice que el método Cualitativa, nos permite recoger datos de forma física y permite profundizar sobre las problemáticas.

2.2. Tipos de investigación

2.2.1. *Investigación descriptiva*

Define a la investigación descriptiva como:

> *La investigación descriptiva consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento. Los resultados de este tipo de investigación se ubican en un nivel intermedio en cuanto a la profundidad de los conocimientos se refiere.* (Fidias, G., 2012, p. 15)

Se refiere a la Investigación Descriptiva a la que:

> *Utiliza criterios sistemáticos que permiten poner de manifiesto la estructura de los fenómenos en estudio, además ayuda a establecer comportamientos concretos mediante el manejo de técnicas específicas de recolección de información. Así, el estudio descriptivo identifica características del universo de investigación, señala formas de conducta y actitudes del universo investigado, descubre y comprueba la asociación entre variables de investigación.* (Méndez, C., 2003, p. 21)

La Investigación Descriptiva mediante el uso de técnicas de recolección de Datos, establece el comportamiento de los mismos, a un nivel intermedio del conocimiento.

2.2.2. *De Campo*

La 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, D., 2008, p. 21)

Esta investigación:

> *La investigación de campo se presenta mediante la manipulación de una variable externa no comprobada, en condiciones rigurosamente controladas, con el fin de describir de*

qué modo o porque causas se produce una situación o acontecimiento particular que se esté investigando. (Graterol, R., 2011, p. 1).

La investigación de campo se presenta por la manipulación de una variable no comprobada, este tipo de información proviene de entrevistas, cuestionarios, encuestas y la observación.

2.3. Población y muestra

La investigación se la desarrollara en la Provincia de Chimborazo, en el Cantón Riobamba, Específicamente en la Ciudad de Riobamba, donde:

2.3.1. *Población*

El Universo o la Población a tratar se presentan del total de empleados que realizan sus funciones dentro de la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo", los que utilizan los equipos Informáticos dentro de la Institución, que en números es un total de 19 personas.

Tabla 1-3: Población de Estudio[1]

DEPARTAMENTOS	NUMERO DE PERSONAS
SISTEMAS	3
FINANCIERO	2
INVERSIONES	4
OPERATIVO	3
GESTION DE RIESGOS	3
GERENCIA	2
PRESIDENCIA	2
TOTAL	19

Fuente: Distributivo del Personal

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

[1] **Nota:** Población aplicada para la Investigación

2.3.2. *Muestra*

El cálculo de la Muestra dentro de este Trabajo de Investigación no se ve necesario porque el Universo es Mínimo y es posible trabajar con el Total.

2.4. Método

3.4.1. *Método Inductivo*

Este método se refiere a:

> *Conocer las características generales o comunes a una diversidad de realidades, tal y como se obtienen a partir del empleo del método comparativo, para articularlas mediante relaciones de causalidad y formular así proposiciones de validez general o leyes científicas generando su valides*. (Calduch, R., 2014, p 33)

Por otro lado: "El método inductivo se aplica en los principios descubiertos a casos particulares, a partir de un enlace de juicios". (Hernández, R., 2010, p. 107)

El método Inductivo permite conocer las características generales a través de las comparaciones para lograr formular la valides de las hipótesis revisadas.

2.5. Técnicas

2.5.1. *Bibliográfica- Documental*

La Técnica bibliográfica-documental es:

> *Se caracteriza por la utilización de documentos; recolecta, selecciona, analiza y presenta resultados coherentes; porque utiliza los procedimientos lógicos y mentales de toda investigación; análisis, síntesis, deducción, inducción, etc., porque realiza un proceso de abstracción científica, generalizando sobre la base de lo fundamental; porque supone una recopilación adecuada de datos que permiten redescubrir hechos, sugerir problemas, orientar hacia otras fuentes de investigación, orientar formas para elaborar ins-trumentos de investigación y elaborar hipótesis.* (Rodríguez, M., 2013, p. 53)

"En un análisis extenso de los documentales biográficos observa las críticas que se le hacen como limitaciones substantivas, metodológicas y teóricas". (Plummer, K., 1989, p. 13)

La investigación Bibliográfica- Documental se caracteriza por la recolección de Documentos, analiza y utiliza los procedimientos lógicos y mentales dentro de toda la investigación.

2.5.2. *Inspección*

La Inspección:

> *Se trata de una exploración física que se realiza principalmente a través de la vista. El objetivo de una inspección es hallar características físicas significativas para determinar cuáles son normales y distinguirlas de aquellas características anormales dentro de los factores o entes de estudio.* (Perez, G., 2009, p. 75)

La inspección implica:

> *Realizar la constatación ocular o la comprobación de un producto, proceso, servicio o instalación —o su diseño— para evaluar su conformidad con unos requisitos en un momento determinado". Con lo anterior revisado la Inspección permite a través de una exploración de forma física determinar cuáles son las características normales y anormales para que cumplan los requisitos necesarios y continúen en su proceso de*

elaboración o transformación. (International Laboratory Accreditation Cooperation., 2016)

2.5.3. *Matriz FODA o Matriz DAFO*

Es una:

> *Herramienta estratégica de análisis de la situación de la empresa. El principal objetivo de aplicar la matriz dafo en una organización, es ofrecer un claro diagnóstico para poder tomar las decisiones estratégicas oportunas y mejorar en el futuro. Su nombre deriva del acrónimo formado por las iniciales de los términos: debilidades, amenazas, fortalezas y oportunidades. La matriz de análisis dafo permite identificar tanto las oportunidades como las amenazas que presentan nuestro mercado, y las fortalezas y debilidades que muestra nuestra empresa.* (Espinosa, R. 2019, p. 65)

El análisis FODA

> *Es un instrumento de planificación estratégica, por lo general se usa como parte de hacer una exploración del entorno, que ayudan a identificar los factores externos que deben ser previsto, y los factores internos fortalezas y debilidades es decir que necesitan ser planificadas en la determinación de que una empresa de ir en el futuro.* (Chiavenato, I., 2000, p. 35)

La matriz FODA permite una exploración del entorno el cual ayuda a identificar los factores externos y los factores internos para determinar el futuro de la empresa.

2.6. Instrumentos

2.6.1. *El Cuestionario*

El cuestionario:

> *Es un procedimiento considerado clásico en las ciencias sociales para la obtención y registro de datos. Su versatilidad permite utilizarlo como instrumento de investigación y como instrumento de evaluación de personas, procesos y programas de formación. Es una técnica de evaluación que puede abarcar aspectos cuantitativos y cualitativos. Su característica singular radica en que para registrar la información solicitada a los mismos sujetos, ésta tiene lugar de una forma menos profunda e impersonal, que el "cara a cara" de la entrevista. Al mismo tiempo, permite consultar a una población amplia de una manera rápida y económica.* (Azofra, M., 1999, p. 2).

Además es:

> *El cuestionario: este instrumento se utiliza, de un modo preferente, en el desarrollo de una investigación en el campo de las ciencias sociales: es una técnica ampliamente aplicada en la investigación de carácter cualitativa generando un análisis básico y necesario de los objetos*. (Osorio, R., 1990, p. 84)

El cuestionario es un instrumento que permite registrar la información de la población de estudio para obtener información cualitativa o cuantitativa

2.6.2. *La Observación*

La Observación es:

> *Una técnica que consiste en observar atentamente el fenómeno, hecho o caso, tomar información y registrarla para su posterior análisis. La observación es un elemento fundamental de todo proceso investigativo; en ella se apoya el investigador para obtener el mayor número de datos. Gran parte del acervo de conocimientos que constituye la ciencia a sido lograda mediante la observación.* (Hernandez, R., 2010, p. 24)

La Observación es: “Un proceso en el cual se obtiene información mediante el uso de los sentidos”. Según los autores la observación es un elemento que permite obtener los datos

necesarios a través del uso de los sentidos". (Raffino, M., 2020, p. 15)

2.6.3. Inventarios

Los Inventarios son:

> *Bienes reales y concretos, es decir bienes muebles e inmuebles. Éstos forman el caudal comercial de una persona o de una empresa. Dichos bienes son para vender, de ahí el carácter de comercial, o para consumición de bienes y/o servicios. Los inventarios se realizan en un período determinado de tiempo.* (Raffino, M., 2020, p. 73)

Según), Inventario es:

> *Uno de los conceptos más importantes para la gestión y administración de una empresa, ya que gracias a ellos podemos conocer la situación real de la empresa. Esta palabra hace referencia a los productos que posee la empresa, pero también a la acción de hacer un inventario en la empresa para el control de que existe ningún problema grave en la empresa*. (Caurin, J., 2018, p. 19)

Los Inventarios permiten conocer la situación real de la empresa, es decir que son los productos que posee la empresa, además es un control concreto.

2.7. Análisis e interpretación de resultados

2.7.1. ***Cuestionario aplicado***

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

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

¿Con que frecuencia Ud. cambian las claves de acceso al sistema y/o equipo?

( ) Mensual ( ) Trimestral ( ) Semestral ( ) Anual ( ) Nunca

¿Conoce Usted las medidas de seguridad física implementadas por el área de sistemas del COAC??

Si ( ) No ( )

¿Conoce usted si existen políticas para la seguridad para proteger al sistema informáticos de COAC?

Si ( ) No ( )

¿A su criterio el equipo informático que usted utiliza le ayuda a cumplir sus actividades laborales en una forma:

( ) Excelente ( ) Bueno ( ) Regular ( ) Malo

¿Las condiciones eléctricas para el funcionamiento de del sistema informático del COAC considera usted que son?:

( ) Excelente ( ) Bueno ( ) Regular ( ) Malo

¿El Sistema Informático que utiliza actualmente el COAC para el manejo de la Información, es:

( ) Excelente ( ) Bueno ( ) Regular ( ) Malo

¿Conoce usted si existe un plan de mantenimientos para los equipos informáticos del COAC?

( ) Bastante ( ) Poco ( ) Nada

¿Existe una comunicación previa cuando va existir cambios que los equipos informáticos?

Si ( ) No ( )

¿La información que Ud. generar en el sistema informáticos del COAC lo guarda en?

( ) Propia PC ( ) Disco externo ( ) Unidades de almacenamiento ( ) Nube

¿Conoce usted si se ha socializado el plan de contingencia del COAC en caso de algún Tipo de Riesgo?

Si ( ) No ( )

GRACIAS POR SU COLABORACIÓN

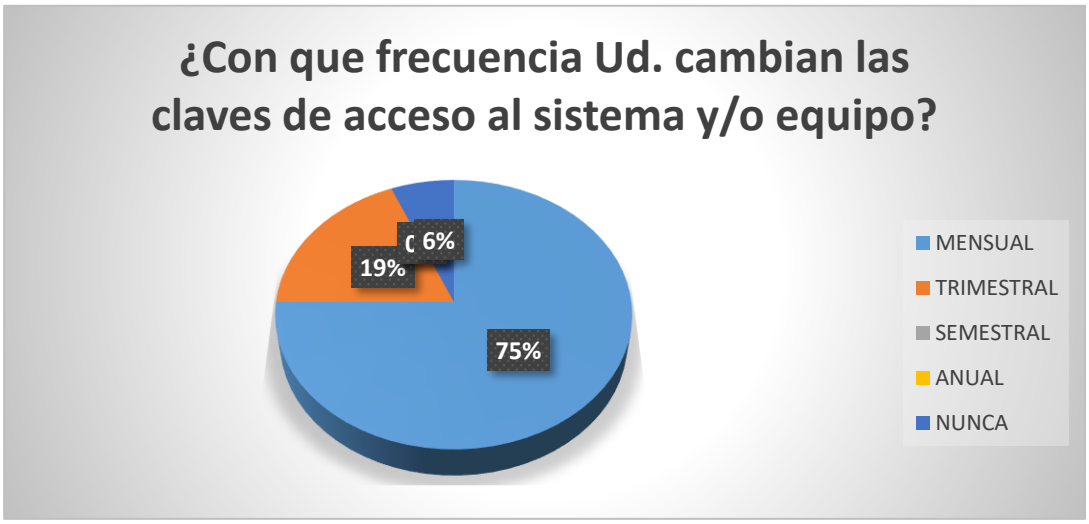
2.7.2. *Análisis del Cuestionario*

Tabla 2-3: Pregunta N° 1[2]

	MENSUAL	TRIMESTRAL	SEMESTRAL	ANUAL	NUNCA	TOTAL
1. **¿Con que frecuencia Ud. cambian las claves de acceso al sistema y/o equipo?**	**12**	**3**	**0**	**0**	**1**	16
PORCENTAJE	75,00%	18,75%		0,00%	6,25%	100%

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020



Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Gráfico 1-3: Pregunta N° 1

Análisis: En relación a la pregunta N° 1: ¿Con que frecuencia Ud. cambian las claves de acceso al sistema y/o equipo?; el 75,00% de los encuestados es decir 12 empleados cambian las claves de acceso ya que el sistema les solicita el cambio de manera mensual, el 18,75% de los encuestados es decir 3 empleados el sistema les solicita el cambio de manera trimestral, por último el 6,25% de los encuestados es decir 1 empleado no cambia las claves de acceso ya que no tiene acceso a la misma.

[2] **Nota:** Análisis e interpretación de la pregunta N° 1

Tabla 3-3: Pregunta N° 2[3]

	SI	NO	TOTAL
2. **¿Conoce Usted las medidas de seguridad física implementadas por el área de sistemas del COAC?**	**15**	**1**	16
PORCENTAJE	93,75 %	6,25%	100%

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

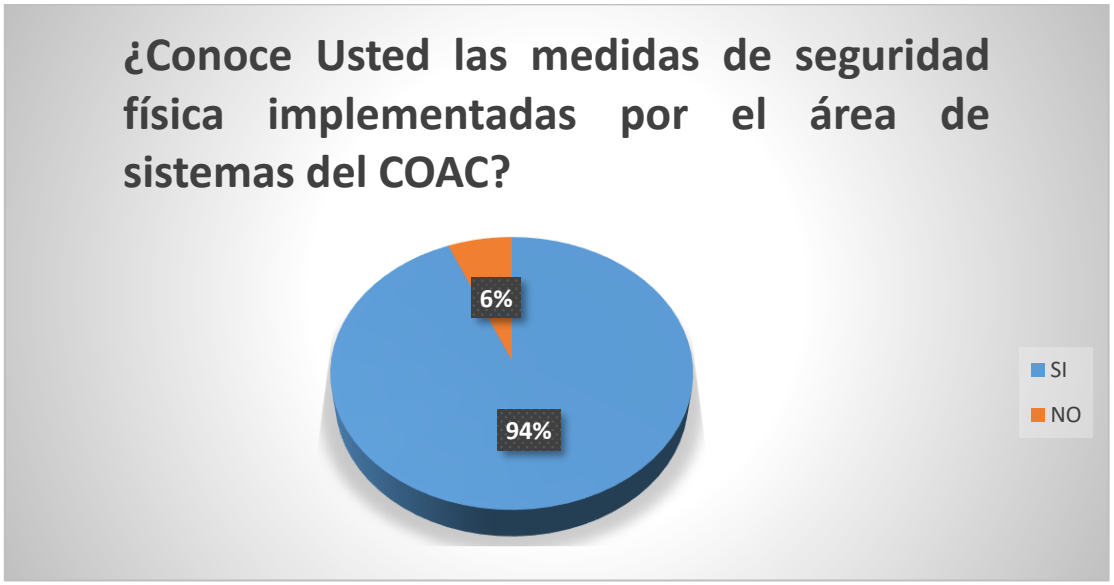


Gráfico 2-3: Pregunta N° 2

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Análisis: En relación a la pregunta N° 2: ¿Conoce Usted las medidas de seguridad física implementadas por el área de sistemas del COAC?; el 93,75% de los encuestados es decir 15 empleados conocen las medidas de seguridad física que implemento el área de Sistemas, por otro lado el 6,25% de los encuestados es decir 1 empleado no conoce las medidas de seguridad física a su totalidad

[3] **Nota:** Análisis e interpretación de la pregunta N° 2

Tabla 4-3: Pregunta N° 3[4]

	SI	NO	TOTAL
3. **¿Conoce usted si existen políticas para la seguridad para proteger al sistema informáticos de COAC?**	**12**	**4**	16
PORCENTAJE	75,00%	25,00%	100%

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

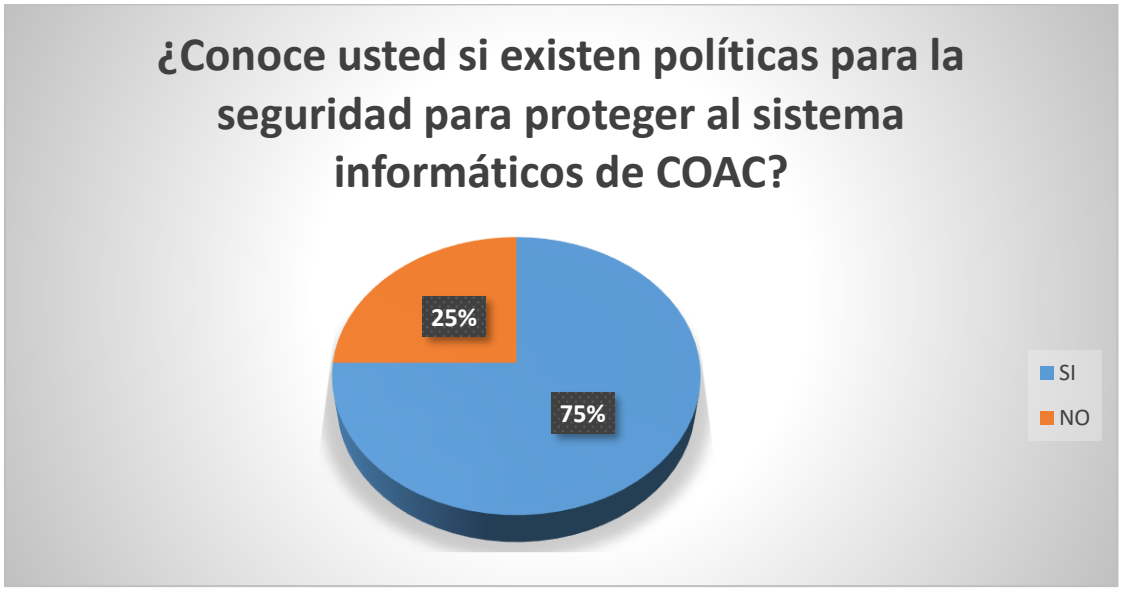


Gráfico 3-3: Pregunta N° 3

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Análisis: En relación a la pregunta N° 3: ¿ Conoce usted si existen políticas para la seguridad para proteger al sistema informáticos de COAC?; el 75,00% de los encuestados es decir 12 empleados las políticas de seguridad para proteger al Sistema Informático, por otro lado el 25,00% de los encuestados es decir 4 empleados no tienen este conocimiento

[4] **Nota:** Análisis e interpretación de la pregunta N° 3

Tabla 5-3: Pregunta N° 4[5]

	EXCELENTE	BUENO	REGULAR	MALO	TOTAL
4. **¿A su criterio el equipo informático que usted utiliza le ayuda a cumplir sus actividades laborales en una forma?**	**7**	**6**	**2**	**1**	16
PORCENTAJE	43,75%	37,5%	12,5%	6,25%	100%

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

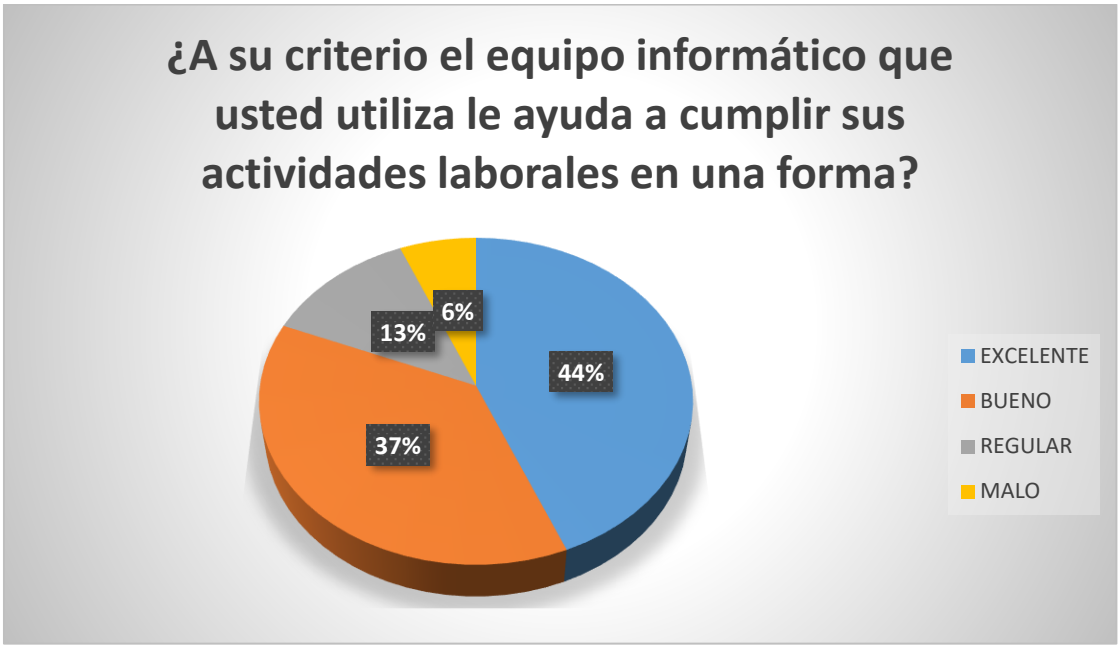


Gráfico 4-3: Pregunta N° 4

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Análisis: En relación a la pregunta N° 4: ¿A su criterio el equipo informático que usted utiliza le ayuda a cumplir sus actividades laborales en una forma?; el 43,75% de los encuestados es decir 7 empleados considera que el equipo informático que utilizan se encuentran en excelentes condiciones debido a que trabajan con equipos adecuados para su labor, el 37,50% de los encuestados es decir 6 empleados comunicaron que sus equipos se encuentran en buenas condiciones para sus labores, el 12,50% de los encuestados es decir 2 empleados dijeron que su equipo se encuentra de una manera regular para su trabajo, por último el 6,25% de empleados es decir 1 empleado dijo que era malo ya que no trabaja con equipos informáticos.

[5] **Nota:** Análisis e interpretación de la pregunta N° 4

Tabla 6-3: Pregunta N° 5[6]

	EXCELENTE	BUENO	REGULAR	MALO	TOTAL
5. **¿Las condiciones eléctricas para el funcionamiento de del sistema informático del COAC considera usted que son?**	**7**	**4**	**1**	**4**	16
PORCENTAJE	43,75%	25,00%	6,25%	25,00%	100%

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

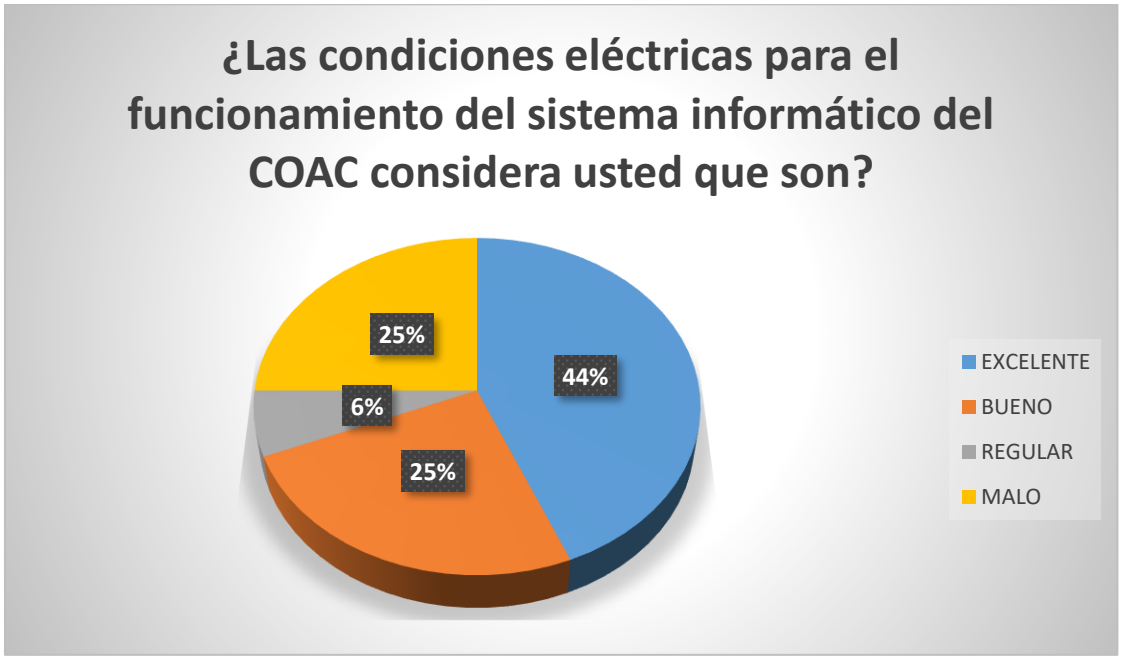


Gráfico 5-3: Pregunta N° 5
Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Análisis: En relación a la pregunta N° 5: ¿Las condiciones eléctricas para el funcionamiento de del sistema informático del COAC considera usted que son?; el 43,75% de los encuestados es decir 7 empleados afirmaron que las condiciones eléctricas se encuentran de una manera excelente, el 25,00% de los encuestados es decir 4 empleados consideran que las condiciones eléctricas se encuentran de buena manera para el funcionamiento informático, el 6,25% de los encuestados es decir 1 empleado dijo que se encuentra de manera regular las condiciones eléctricas, por último el 25,00% de los encuestados es decir 4 empleados considera que las condiciones eléctricas son malas ya que las instalaciones son adecuadas en un edificio Histórico

[6] **Nota:** Análisis e interpretación de la pregunta N° 5

Tabla 7-3: Pregunta N° 6[7]

	EXCELENTE	BUENO	REGULAR	MALO	TOTAL
6. **¿El Sistema Informático que utiliza actualmente el COAC para el manejo de la Información, es?:**	**7**	**5**	**3**	**1**	16
PORCENTAJE	43,75%	31,25%	18,75%	6,25%	100%

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

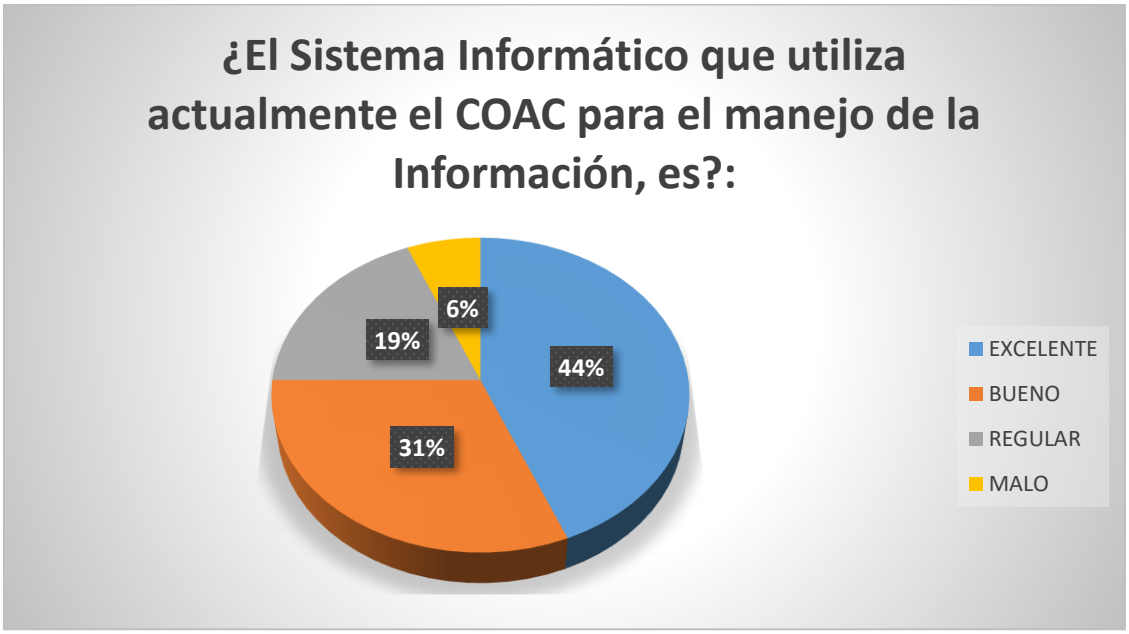


Gráfico 6-3: Pregunta N° 6

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Análisis: En relación a la pregunta N° 6: ¿El Sistema Informático que utiliza actualmente el COAC para el manejo de la Información, es?: el 43,75% de los encuestados es decir 7 creen que el Sistema que utiliza la COAC se encuentra de manera excelente, el 31,25% de los encuestados es decir 5 empleados piensan que el Sistema Informático que se utilizó en la empresa está en una situación buena en su Utilidad, el 18,75% de los encuestados es decir 3 empleados dijeron que se encuentra de manera regular el Sistema para sus funciones, por último el 6,25% de los encuestados es decir 1 empleado comunico que el sistema es malo ya que no lo utiliza.

[7] **Nota:** Análisis e interpretación de la pregunta N° 6

Tabla 8-3: Pregunta N° 7[8]

	BASTANTE	POCO	NADA	TOTAL
7. **¿Conoce usted si existe un plan de mantenimientos para los equipos informáticos del COAC?**	**6**	**7**	**3**	16
PORCENTAJE	37,5%	43,75 %	18,75%	100%

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

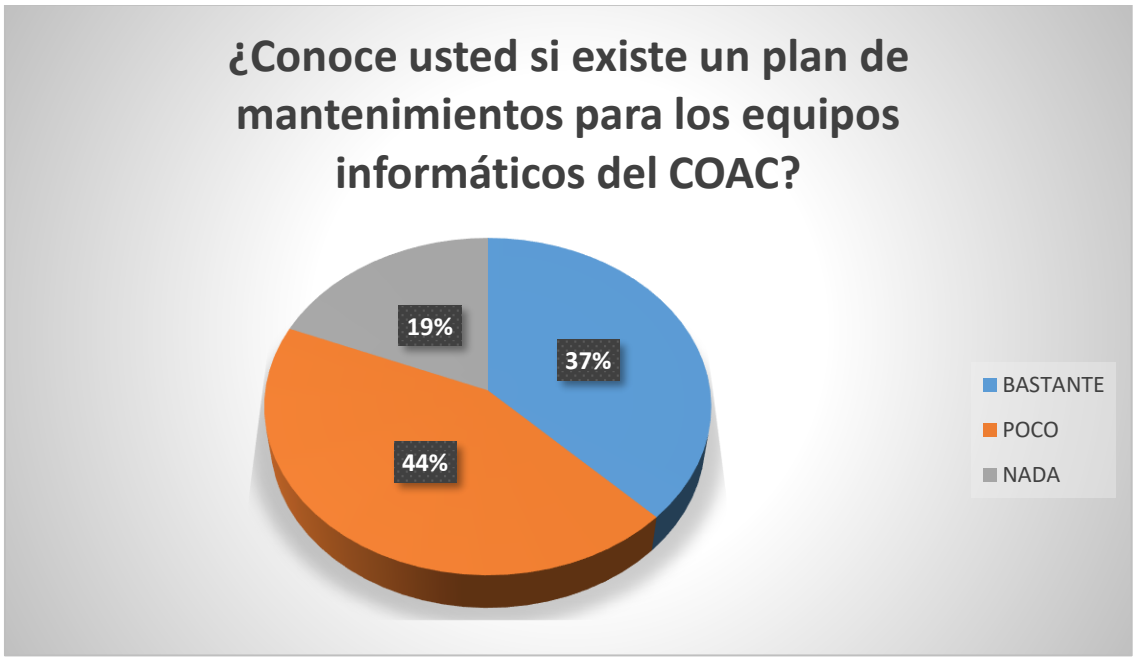


Gráfico 7-3: Pregunta N° 7

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Análisis: En relación a la pregunta N° 7: ¿Conoce usted si existe un plan de mantenimientos para los equipos informáticos del COAC?; el 37,50% de los encuestados es decir 6 empleados comunicaron que tiene un conocimiento bastante amplio en relación al Plan de mantenimiento presente en la COAC, el 43,75% de los encuestados es decir 7 empleados conocen poco sobre el Plan de Mantenimientos para los equipos Informáticos de la COAC, por último el 18,75% de los encuetados es decir 3 empleados no conocen nada del plan ya que casi han necesitado de mantenimientos.

[8] **Nota:** Análisis e interpretación de la pregunta N° 7

Tabla 9-3: Pregunta N° 8[9]

	SI	NO	TOTAL
8. **¿Existe una comunicación previa cuando va existir cambios que los equipos informáticos?**	**12**	**4**	16
PORCENTAJE	75,00%	25,00%	100%

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

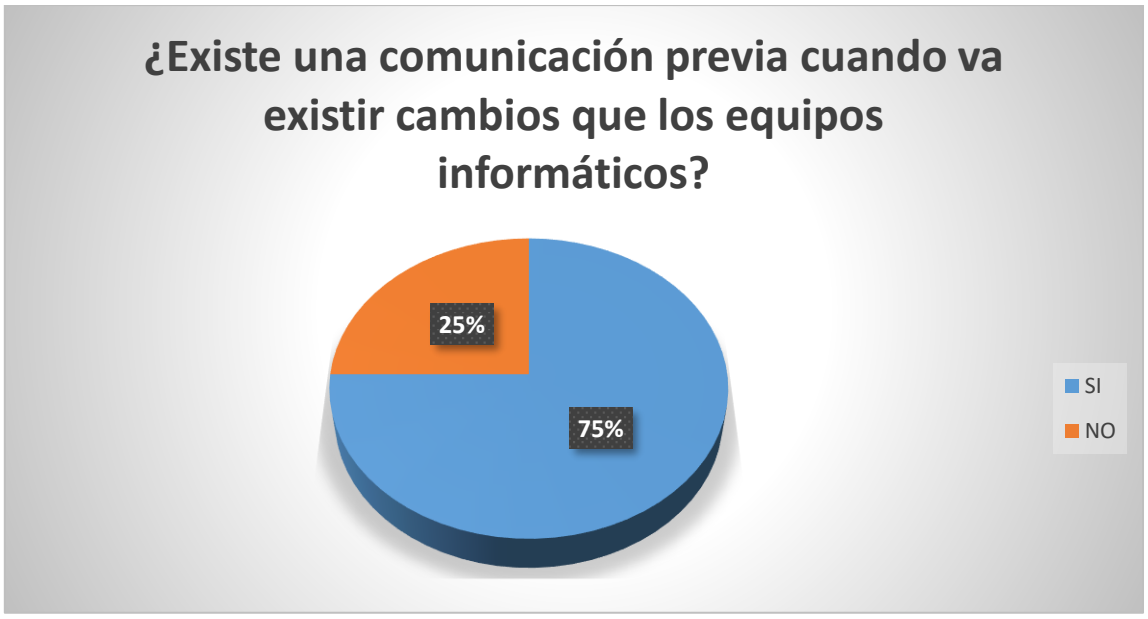


Gráfico 8-3: Pregunta N° 8

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Análisis: En relación a la pregunta N° 8: ¿Existe una comunicación previa cuando va existir cambios que los equipos informáticos?; el 75,00% de los encuestados es decir 12 comunican o se los comunican cuando existe un cambio en los equipos informáticos, por otro lado el 25,00% de los encuestados es decir 4 empleados no se les comunica o comunican si cambian los equipos informáticos

[9] **Nota:** Análisis e interpretación de la pregunta N° 8

Tabla 10-3: Pregunta N° 9[10]

	PROPIA PC	DISCO EXTERNO	UNI. ALMACENAMIENTO	NUBE	TOTAL
9. **¿La información que Ud. generar en el sistema informáticos del COAC lo guarda en?**	**3**	**3**	**2**	**8**	16
PORCENTAJE	18,75%	18,75 %	12,50%	50,00%	100%

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

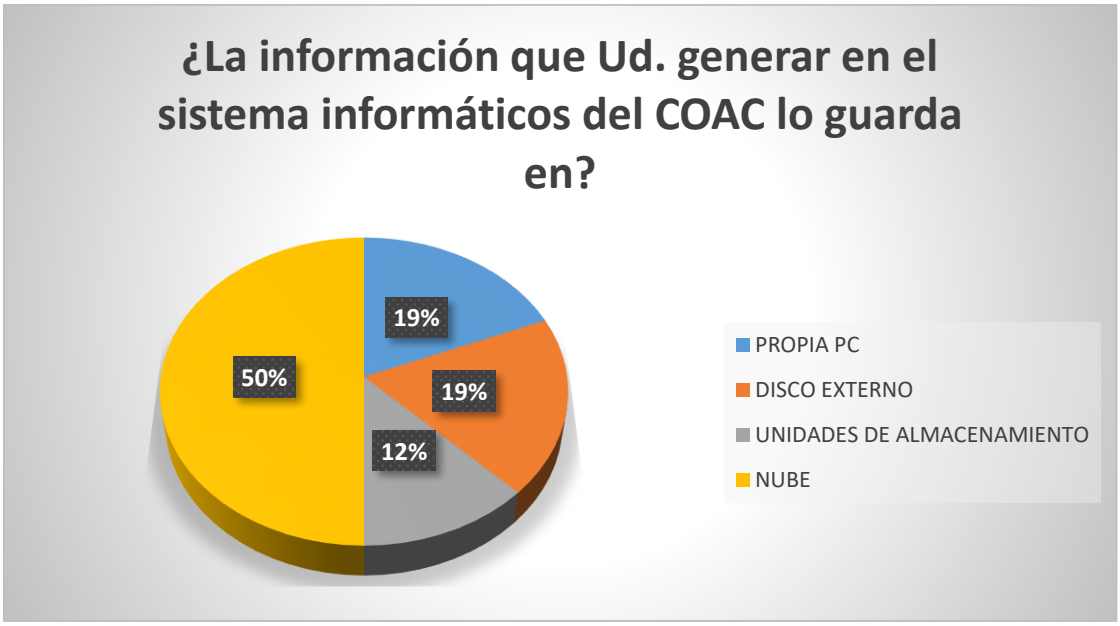


Gráfico 9-3: Pregunta N° 9

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Análisis: En relación a la pregunta N° 9: ¿La información que Ud. generar en el sistema informáticos del COAC lo guarda en?; el 18,75% de los encuestados es decir 3 empleados la información generada la guarda en la propia pc, el 18,75% de los encuestados es decir 3 empleados guarda la información en discos externos, el 12,50% de los encuestados es decir 2 empleados recolecta la información generada en el sistema informático por medio de unidades de almacenamiento, por ultimo 50,00% de los encuestados es decir 8 empleados guardan la información generada a través de la nube

[10] **Nota:** Análisis e interpretación de la pregunta N° 9

Tabla 11-3: Pregunta N° 10[11]

	SI	NO	TOTAL
10. **¿Conoce usted si se ha socializado el plan de contingencia del COAC en caso de algún Tipo de Riesgo?**	**12**	**4**	16
PORCENTAJE	75,00%	25,00%	100%

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

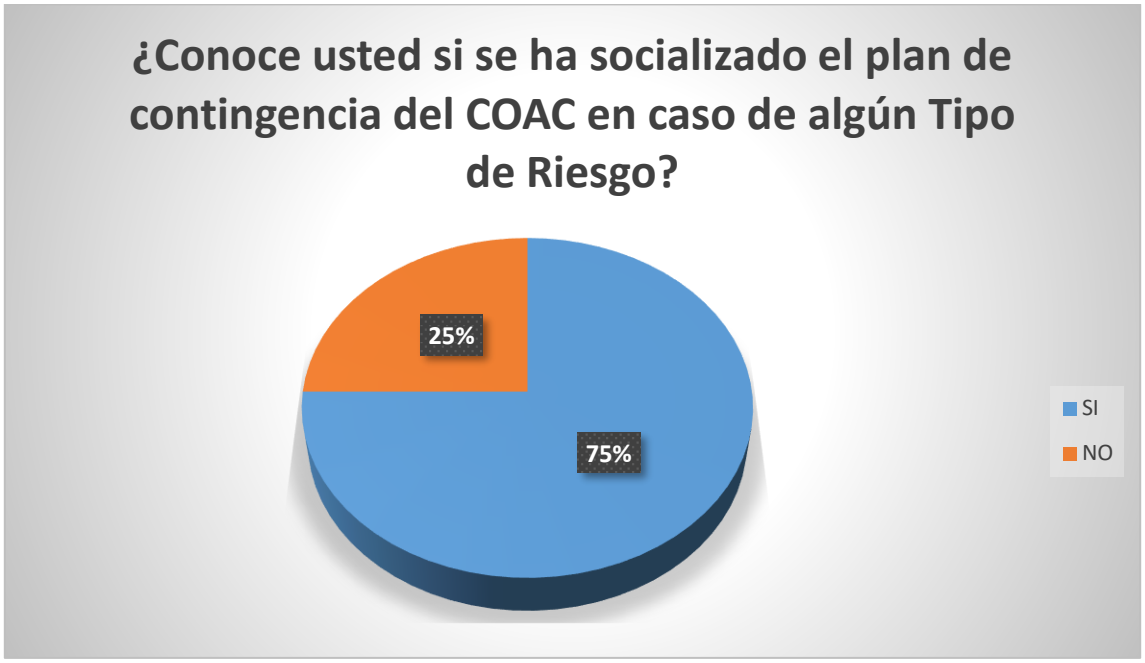


Gráfico 10-3: Pregunta N° 10

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Análisis: En relación a la pregunta N° 10: ¿Conoce usted si se ha socializado el plan de contingencia del COAC en caso de algún Tipo de Riesgo?; el 75,00% de los encuestados es decir 12 empleados le socializado el plan de contingencia, por otro lado el 25,00% de los encuestados es decir 4 empleados no les socializaron el plan de contingencia en caso de Riesgos

[11] **Nota:** Análisis e interpretación de la pregunta N° 10

CAPÍTULO III

3. MARCO DE RESULTADOS Y DISCUSÍON DE RESULTADOS

3.1. Título

AUDITORÍA INFORMÁTICA A LA COOPERATIVA DE AHORRO Y CRÉDITO "EDUCADORES DE CHIMBORAZO" LTDA. DE LA CIUDAD DE RIOBAMBA, PERIODO 2018

3.2. Contenido de la propuesta

Metodología, guía y/o procedimiento

Figura 4-4: COAC "Educadores de Chimborazo"
Fuente: COAC "Educadores de Chimborazo"
Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

FASE I: Planificación de la Auditoría.

FASE II: Ejecución de la Auditoría.

FASE III: Informe de la Auditoría.

FASE I:

Planificación de la Auditoría

3.3. Implementación de la propuesta

3.3.1. *Planificación de la auditoría*

Figura 5-4: COAC "Educadores de Chimborazo"

Fuente: COAC "Educadores de Chimborazo"

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

INSTITUCIÓN:	COOPERATIVA DE AHORRO Y CRÉDITO EDUCADORES DE CHIMBORAZO LTDA.
DIRECCIÓN:	José Veloz 22 – 11 y Eugenio Espejo (Esquina)
NATURALEZA DEL TRABAJO:	Auditoría Informática
PERÍODO:	Año 2018

Figura 6-4: Datos de la Compañía

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

3.3.1.1. *Identificar el origen del trabajo*

La presente Investigación se la desarrollara por ser un requisito necesario para la obtención de su título profesional, además para la Organización como Herramienta de toma de Decisiones Gerenciales y también brindar un Sistema de Evaluación a todos los Procesos.

3.3.1.2. *Hoja de índices y marcas*

PM Auditor y Consultor	**AUDITORÍA INFORMÁTICA** **HOJA DE ÍNDICES Y MARCAS** **ARCHIVO PERMANENTE**	**HIM 1/2**

MARCA	**SIGNIFICADO**
✓	Verificado
	Comparado con documentos
	Comparado con inventario
©	Pendiente de chequear
¿?	Confirmar preguntas
	Resultados
	Comentario
*	Observación
	No coinciden los datos
PASL	Programa de Auditoría Seguridad Lógica
CCISL	Cuestionario de Control Interno Seguridad Lógica
PASF	Programa de Auditoría Seguridad Física
CCISF	Cuestionario de Control Interno Seguridad Física
PATC	Programa de Auditoría Tecnologías de la Información y Comunicación
CCITIC	Cuestionario de Control Interno Tecnologías de la Información y Comunicación
PAGI	Programa de Auditoría Gestión Informática
CCIE	Cuestionario de Control Interno Empleados
AFODA	Análisis FODA
MCFO	Matriz de Correlación FO
MCDA	Matriz de Correlación DA
MPRI	Matriz de Prioridades
PE	Perfil Estratégico
HH	Hoja de hallazgos
HIM	Hoja de índices y marcas
DP	Datos Preliminares
PSP	Propuesta de Servicios Profesionales
MH	Matriz de Hallazgos

Elaborado por: P.A.M.G	**Fecha:** 2019-11-27
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-11-27

	AUDITORÍA INFORMÁTICA HOJA DE ÍNDICES Y MARCAS ARCHIVO PERMANENTE	HIM 2/2

MARCA	SIGNIFICADO
OT	Orden de Trabajo
CC	Carta Compromiso
CT	Contrato de Trabajo
NI	Notificación de Inicio de la Auditoría
SDA	Solicitud de Auditoría
PGA	Programa General de Auditoría
PA	Presupuesto General
CPIF	Carta de Presentación Informe Final
IF	Informe Final
P.A.M.G	Paúl Alejandro Merizalde Guamanzara
H.B.V.S	Hítalo Bolívar Veloz Segovia
W.G.Y.C	William Geovanny Yanza Chávez
CACECH	Cooperativa de Ahorro y Crédito "Educadores de Chimborazo Ltda."
≡	Congruente-Igual a

Elaborado por: P.A.M.G	**Fecha:** 2019-11-27
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-11-27

3.3.1.3. *Programa general de auditoría*

	AUDITORÍA INFORMÁTICA PROGRAMA GENERAL DE AUDITORÍA ARCHIVO PERMANENTE	**PGA 1/1**

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

Objetivos

General:

- Evaluar la efectividad de los procesos referentes a los sistemas informáticos, usando COSO 2 y las Normas ISO 27002 para obtener un análisis necesario para lograr obtener los hallazgos de la auditoria

Específicos:

- Comprobar el manejo adecuado del equipo informático de la entidad a fin de asegurar economía en los resultados entregados por la empresa.
- Evidenciar si la seguridad se encuentra de forma razonable en el manejo de los recursos disponibles en la empresa.
- Identificar el control interno en la empresa para cuantificarlo según el COSO 2.
- Analizar los sistemas informáticos para determinar debilidades y fortalezas de los mismos.
- Presentar el informe dando a conocer los resultados, conclusiones y recomendaciones a la organización.

N.	PROCEDIMIENTO	REF. P/T	ELAB. POR	FECHA	OBSERVACIONES
1	Proceda con el levantamiento de la información	DP	PAMG	2019-11-05	---
2	Presente la Propuesta de Servicios Profesionales	PSP	PAMG	2019-11-05	---
3	Genere la carta de notificación de inicio de la auditoría	CC	PAMG	2019-11-08	---
4	Realice la auditoría	OT	PAMG	2019-11-10	---
5	Realice el borrador del informe para revisión	CT	PAMG	2019-12-30	---
6	Redacte el informe final	NI	PAMG	2020-01-19	---
7	Presente el informe con los comentarios y Sugerencias necesarias.	IF	PAMG	2020-01-27	---
Elaborado por: P.A.M.G			**Fecha:** 2019-11-25		
Revisado por: W.G.Y.C H.B.V.S			**Fecha:** 2019-11-25		

	AUDITORÍA INFORMÁTICA INFORMACIÓN GENERAL ARCHIVO PERMANENTE	**DP 1/5**

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

ANTECEDENTES

El 26 de junio de 1964 se creó la Cooperativa de Ahorro y Crédito Educadores de Chimborazo, CACECH; es una Institución financiera Cooperativista de carácter de Gremio exclusivo, con más de 4000 socios quienes pertenecen al Magisterio de la provincia de Chimborazo, realizan aportaciones mensuales que les permite gozar de servicios adicionales como descuentos, seguro de vida, entre otros con empresas con la que la Cooperativa tiene convenios.

Entre los productos financieros que ofrece la COAC se encuentra: Libretas de Libre Ahorro – Libre Retiro; Libreta de Ahorro Cautivo y Fondos de Reserva; Inversiones a plazo fijo con el mejor interés en el mercado; permitiendo a los socios de la Cooperativa, el acceso a créditos como: Anticipo de Sueldo, Emergencia, Ordinario, y CREDIFLASH, conforme a su necesidad y capacidad de pago, con un monto máximo de 20.000 dólares.

Referente a la Dirección esta entidad financiera se encuentra ubicada en el centro histórico la ciudad de Riobamba, capital de la provincia de Chimborazo, en las calles Veloz y Espejo; cuyas instalaciones se encuentran en un edificio de su propiedad, el horario de atención es de Lunes a Viernes de 09:00 a 16:00 sin cerrar a medio día, y Sábados desde las 08:00 a 13:00.

La Cooperativa realiza agasajos a sus socios como entrega de regalos en fechas importantes y además sortea dos automóviles 0 KM en el transcurso del año, el primero en el mes de Julio y el segundo en Diciembre, además en el mes de Diciembre entrega a los socios con mayores movimientos en la cuenta, regalos especiales y el aguinaldo navideño.

Como otro servicio que cuenta la institución es la tarjeta de débito Visa Electrón CACECH, con esta tarjeta se puede realizar pagos de los fondos disponibles en la cuenta, a través de la tarjeta se accede al sueldo que se deposita de manera mensual en cada una de las cuentas por el Sistema de Pagos Interbancarios del Banco Central, el cual es la manera más rápida dentro del sector financiero.

Elaborado por: P.A.M.G	**Fecha:** 2019-11-25
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-11-25

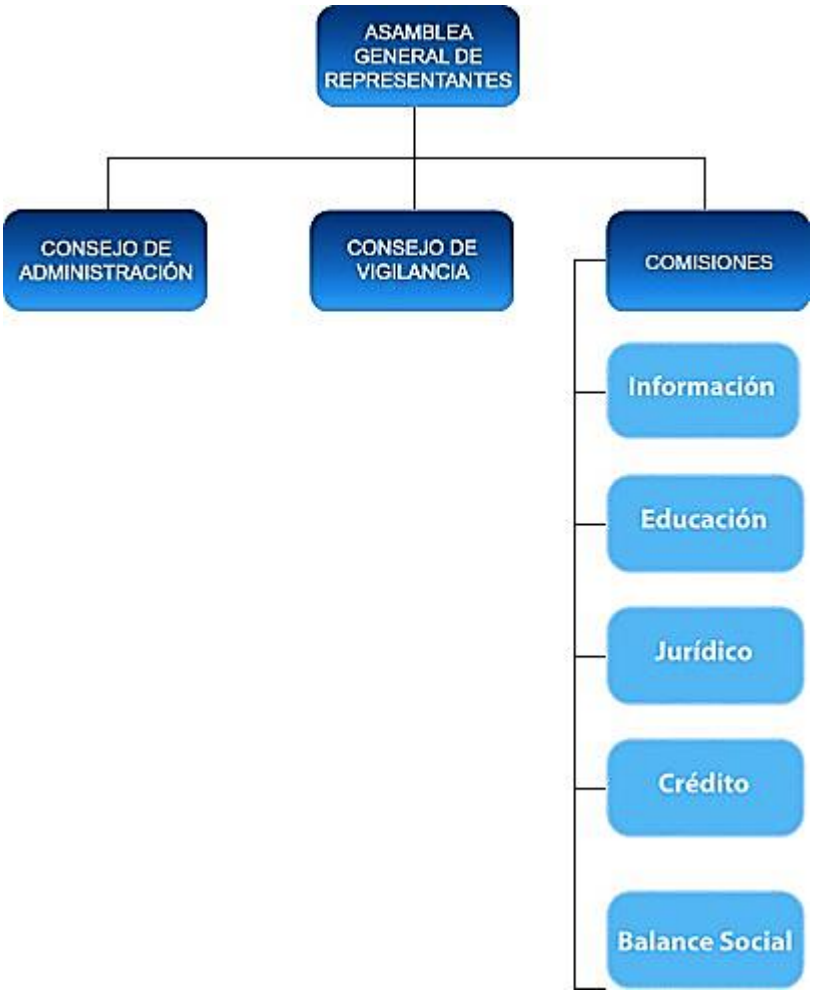


Figura 7-4: Gobierno Cooperativo

Fuente: coaceducadoreschimborazo

Recuperado de: http://www.coaceducadoreschimborazo.fin.ec/, 2020

	AUDITORÍA INFORMÁTICA INFORMACIÓN GENERAL ARCHIVO PERMANENTE	**DP 3/5**

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

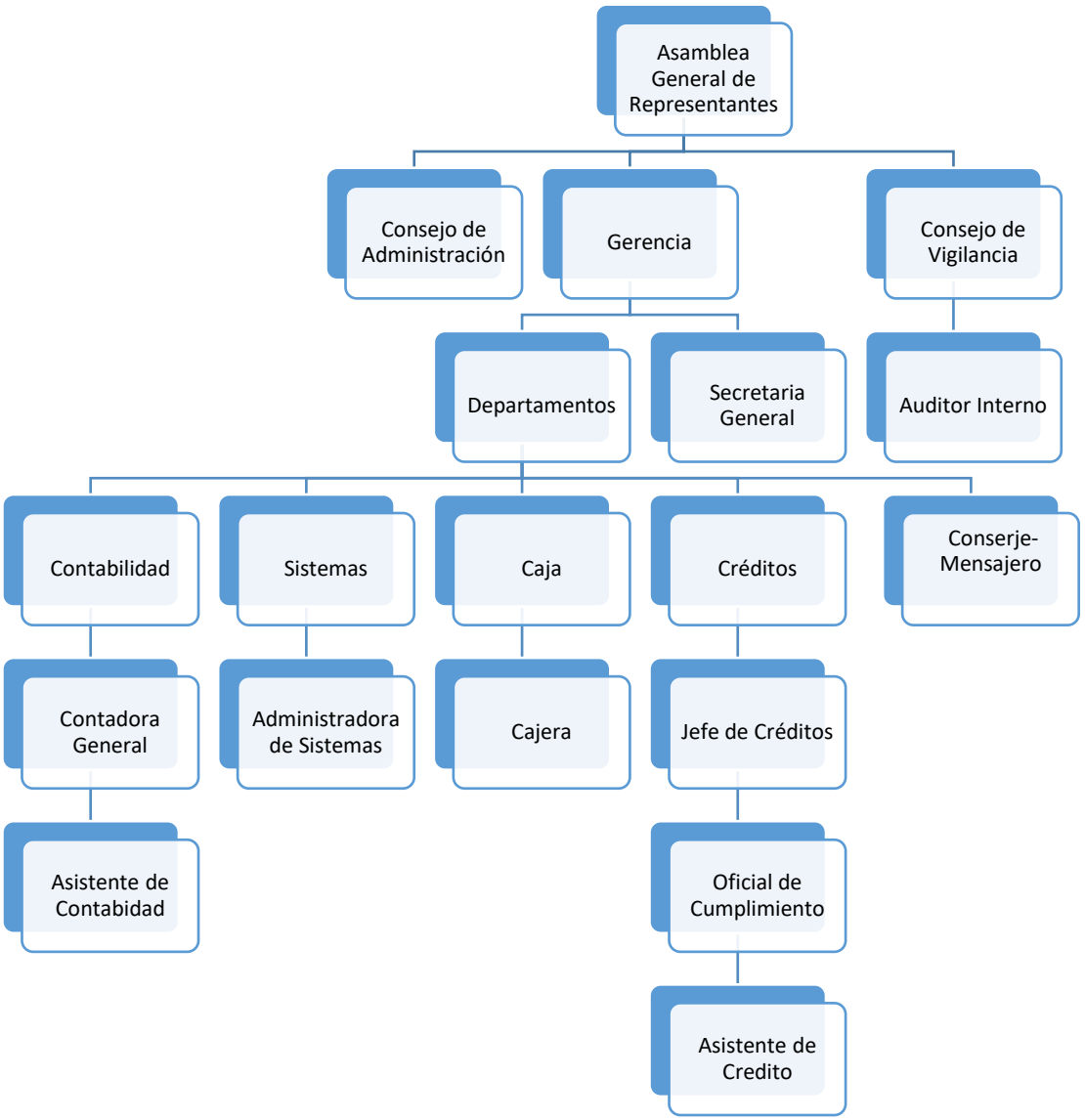


Figura 8-4: Organigrama Estructural

Fuente: coaceducadoreschimborazo

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Elaborado por: P.A.M.G	**Fecha:** 2019-11-25
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-11-25

	AUDITORÍA INFORMÁTICA **INFORMACIÓN GENERAL** **ARCHIVO PERMANENTE**	**DP 4/5**

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

UBICACIÓN

País	Ecuador
Provincia	**Chimborazo**
Cantón	**Riobamba**
Ciudad	**Riobamba**
Dirección	**Calle Espejo y Veloz Esq.**

Figura 9-4: Ubicación

Fuente: Cooperativa de Ahorro y Crédito Educadores de Chimborazo

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Figura 10-4: Instalaciones

Fuente: google.com/maps/

Extraído de: https://www.google.com/maps/@-1.6721284,-78.6483592,3a,75y,260.4h,90.78t/data=!3m6!1e1!3m4!1sOLaHTm1xWfouOSWFhyyK7g!2e0!7i13312!8i6656, 2020

Elaborado por: P.A.M.G	**Fecha:** 2019-11-25
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-11-25

	AUDITORÍA INFORMÁTICA INFORMACIÓN GENERAL ARCHIVO PERMANENTE	**DP 5/5**

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

Figura 11-4: Dirección

Fuente: google.com/maps/

Extraído de: https://www.google.com/maps/@-1.6721284,-78.6483592,3a,75y,260.4h,90.78t/data=!3m6!1e1!3m4!1sOLaHTm1xWfouOSWFhyyK7g!2e0!7i13312!8i6656, 2020

Elaborado por: P.A.M.G	**Fecha:** 2019-11-25
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-11-25

	AUDITORÍA INFORMÁTICA PROPUESTA DE SERVICIOS PROFESIONALES ARCHIVO PERMANENTE	**PSP 1/1**

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

Riobamba, 5 de noviembre de 2019

Ingeniero

Ramiro Fabián Tobar Esparza

GERENTE GENERAL

Presente.-

De mi consideración:

Agradecemos la oportunidad de presentar nuestra propuesta de **AUDITORÍA INFORMÁTICA A LA COOPERATIVA DE AHORRO Y CRÉDITO "EDUCADORES DE CHIMBORAZO" LTDA. DE LA CIUDAD DE RIOBAMBA, PERIODO 2018.**

La propuesta de servicios ha sido elaborada para que conozca las respuestas a los requerimientos, con forme al alcance de la Auditoría Informática, las Normas COSO 2, NORMAS ISO 27002.

Le informamos que la empresa asegura el compromiso personal de entregarles un informe de auditoría eficiente y de la manera más profesional, logrando una relación a corto y largo plazo de confianza, logrando recomendaciones para mejorar el servicio.

La acción de control se realizara de acuerdo con las condiciones legales, normas internacionales, estas normas requieren que el examen sea planificado y ejecutado para obtener la certeza razonable de que la información y la documentación examinada no contienen exposiciones erróneas de carácter significativo, igualmente que las operaciones a las cuales corresponden se hayan ejecutado de conformidad a las disposiciones legales y reglamentarias vigentes, además se evaluará el control interno y se determinará la falencias y mejorarlas a través de evidencias para elaborar el informe de Auditoria a través de las conclusiones y recomendaciones a ser utilizadas por la administración para tomar decisiones concretas dentro de la Cooperativa.

Agradezco la atención prestada y cuento con su aprobación.

Atentamente

Paúl Alejandro Merizalde Guamanzara
Auditor Independiente

Elaborado por: P.A.M.G	**Fecha:** 2019-11-25
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-11-25

	AUDITORÍA INFORMÁTICA CONTRATO POR PRESTACIÓN DE SERVICIOS DE AUDITORÍA ARCHIVO PERMANENTE	**CT 1/2**

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

CONTRATO DE PRESTACION DE SERVICIOS PROFECIONALES

Siendo el Día Lunes 11 de Noviembre de 2019, comparecen a la celebración del presente contrato por una parte la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda., encontrándose domiciliada en la Provincia de Chimborazo, en la ciudad de Riobamba, la cual se encuentra representada actualmente por el Ing. Ramiro Fabián Tobar Esparza a quien para efectos del presente contrato se le denominara **CONTRATANTE**; y por otra parte, el auditor Paúl Alejandro Merizalde Guamanzara con C.I.: 17171551282-6, Gerente General de PM Auditor y Consultor, con domicilio principal en la ciudad de Riobamba, quien para efectos del presente contrato se le denominara **CONTRATISTA**; hemos celebrado el contrato de prestación de servicios profesionales de **Auditoría Informática** que se regirá por las siguientes cláusulas:

Primera – Objeto: El **CONTRATISTA** de PM Auditor y Consultor se obligan a cumplir la labor de Auditoría Informática de la Cooperativa de Ahorro y Crédito Educadores de Chimborazo Ltda., por el período económico 2018, 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 noviembre del 2019, que para el efecto de descripción de funciones se considera incorporada al presente contrato.

Segunda – Duración: El presente contrato tendrá vigencia de tres meses, comprendido desde el mes de noviembre de 2019 hasta el mes de enero de 2020, 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 de 2018. No obstante lo anterior, el **CONTRATISTA** de PM Auditor y Consultor 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 séptima de este contrato.

Tercera – Obligaciones del Contratante: Además de las obligaciones generales derivadas del presente contrato, el Contratante se compromete a a) Prestarle toda colaboración que solicite el **CONTRATISTA** de PM Auditor y Consultor facilitándole 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 al el **CONTRATISTA** de PM Auditor y Consultor con no menos de cinco (5) días hábiles de anticipación a la fecha de vencimiento de su presentación.

Cuarta – Valor y Forma de Pago: El contratante no reconocerá a el **CONTRATISTA** de PM Auditor y Consultor, 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.

Quinta – Obligaciones de los Contratistas Independientes: El **CONTRATISTA** de PM Auditor y Consultor 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 Informática.

Sexta – Lugar de Presentación del Servicio: El servicio contratado por el **CONTRATANTE** se prestará específicamente en las instalaciones de la empresa, la misma se encuentra en la ciudad de Riobamba.

Elaborado por: P.A.M.G	**Fecha:** 2019-11-30
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-11-30

	AUDITORÍA INFORMÁTICA CONTRATO POR PRESTACIÓN DE SERVICIOS DE AUDITORÍA ARCHIVO PERMANENTE	**CT 2/2**

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

Séptima – 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 meses pactado, en cualquier momento, pagando a el **CONTRATISTA** de PM Auditor y Consultor el precio total acordado en la cláusula Cuarta, el aviso de determinación del contrato debe ser dado a los contratistas independientes por lo menos con treinta días calendario de anticipación a la fecha efectiva de dicha terminación.

Octava – Dotaciones y Recursos: El **CONTRATANTE** facilitará a su coste a el **CONTRATISTA** de PM Auditor y Consultor el espacio físico, así como los elementos necesarios requeridos para el desempeño de su labor, tales como equipo de cálculo, mesas, sillas, etc.

Novena – Autonomía de PM Auditor y Consultor: En el desarrollo del presente contrato de prestación de servicios profesionales de Auditoría Informática, **CONTRATISTA** de PM Auditor y Consultor actúa como tal, realizando la labor encomendada con libertad y autonomía técnica y directiva.

Décima – 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.

Otros: Las partes dejan constancia 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, lunes 11 de noviembre de 2019.

El **CONTRATANTE** **CONTRATISTA** de PM Auditor y Consultor

Ing. FABIÁN TOBAR ESPARZA MSc.
Gerente General CACECH

PAÚL ALEJANDRO MERIZALDE
Auditor Independiente

Elaborado por: P.A.M.G	**Fecha:** 2019-11-30
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-11-30

	AUDITORÍA INFORMÁTICA NOTIFICACIÓN DE INICIO DE LA AUDITORÍA ARCHIVO PERMANENTE	**NI**

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

Riobamba, 12 de noviembre de 2019

Ingeniero

Ramiro Fabián Tobar Esparza

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 PM Auditor y Consultor, se encuentra realizando la Auditoría Informática, por el período comprendido entre el 1 de enero al 31 de diciembre de 2018.

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

Atentamente,

Paúl Alejandro Merizalde Guamanzara
Gerente de PM Auditor y Consultor

Elaborado por: P.A.M.G	**Fecha:** 2019-11-30
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-11-30

	AUDITORÍA INFORMÁTICA SOLICITUD DE AUDITORÍA ARCHIVO PERMANENTE	**SDA**

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

COOPERATIVA DE AHORRO Y CRÉDITO
"EDUCADORES DE CHIMBORAZO" LTDA.
RIOBAMBA - ECUADOR
SEPS-ROEPS - 2013 - 000119

Cada Día más GRANDE!!!

CERTIFICADO

El suscrito Gerente General **Ing. FABIÁN TOBAR ESPARZA,** de la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda., y a petición verbal de la parte interesada tiene a bien certificar que:

El **Señor PAÚL ALEJANDRO MERIZALDE GUAMANZARA,** con cédula de ciudadanía N° 171551282-6, estudiante de la Escuela Superior Politécnica de Chimborazo, de la Facultad de Administración de Empresas, Escuela de Contabilidad y Auditoría, realizara su **Trabajo de Titulación** con el TEMA: **AUDITORÍA INFORMÁTICA AL ÁREA DE SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO "EDUCADORES DE CHIMBORAZO" LTDA. DE LA CIUDAD DE RIOBAMBA, PERIODO 2018.**

Es todo cuanto puedo informar en honor a la verdad, autorizo al interesado hacer uso del presente para trámites estudiantiles.

Riobamba julio 8, 2019

Ing. FABIÁN TOBAR ESPARZA
Gerente General CACECH
VILMA O.

COOPERATIVA DE AHORRO Y CRÉDITO CACECH GERENCIA EDUCADORES DE CHIMBORAZO LTDA.

Dirección: Veloz 22 - 11 y Espejo (esquina) Telefax: 2961 473 - Telfs.: (03) 2942 893 - 2969271
www.coaceducadoreschimborazo.fin.ec E-mail: cacech@hotmail.com

Elaborado por: P.A.M.G	**Fecha:** 2019-11-30
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-11-30

3.3.1.4. *Componentes consideradas para la evaluación*

Para el desarrollo de la evaluación se construirá en base lo que está dentro de las Referencias de Procesos de COSO II, los cuales son:

Ambiente Interno

Establecimiento de Objetivos

Identificación de Eventos

Evaluación de Riesgos

Respuesta al Riesgo

Actividades de Control

Información y Comunicación

Monitoreo

3.3.1.5. *Plan de auditoría*

	AUDITORÍA INFORMÁTICA PLAN DE AUDITORÍA ARCHIVO CORRIENTE	PGA 1/2

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

No.	Actividad	Responsable	Semanas															
			OCT 1	OCT 2	OCT 3	OCT 4	NOV 1	NOV 2	NOV 3	NOV 4	DIC 1	DIC 2	DIC 3	DIC 4	ENE 1	ENE 2	ENE 3	ENE 4
1	Elaborar planificación de auditoría	Paúl Merizalde																
2	Aprobar planificación de auditoría	Ing. William Yanza Ing. Hítalo Veloz																
3	Preparar instrumentos	Paúl Merizalde																
4	Realizar visita preliminar	Paúl Merizalde																
5	Iniciar auditoría	Paúl Merizalde																
6	Auditar las TIC de la Entidad	Paúl Merizalde																
10	Presentar borrador del Informe	Paúl Merizalde																
11	Emitir informe final	Paúl Merizalde																
12	Comunicar resultados	Paúl Merizalde																

Elaborado por: P.A.M.G	**Fecha:** 2019-12-01
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-01

3.3.1.6. *Presupuesto*

	AUDITORÍA INFORMÁTICA **PRESUPUESTO GENERAL** **ARCHIVO CORRIENTE**	**PGA 2/2**

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

No.	**Artículo**	**Cantidad**	**Unidad**	**Costo**	**Total**
1	Honorarios profesionales	-	-	-	0,00
2	Computador*	1	Unidades	500,00	500,00
3	Impresora*	1	Unidades	225,00	225,00
4	Celular*	1	Unidades	210,00	210,00
5	Calculadora*	1	Unidades	15,00	15,00
6	Unidad Flash USB*	1	Unidades	5,00	5,00
7	Cuaderno Universitario	1	Unidades	1,45	1,45
8	Hojas papel bond tamaño A4	3	Resmas	3,00	9,00
9	Lápiz HB	5	Unidades	0,30	1,50
10	Esferos (Azul, Rojo)	4	Unidades	0,30	1,20
11	Borrador	3	Unidades	0,20	0.60
12	Resaltador	1	Unidades	0,75	0,75
13	Transporte	20	Veces	0,30	6,00
14	Protector de documentos	15	Unidades	0,20	3,00
15	Carpetas (Azul y Rojo)	2	Unidades	0,75	1,50
16	Impresiones	400	Unidades	0,05	20,00
	TOTAL				***$ 1000,00***

(*) Los artículos adquiridos no se encuentran en un estado exclusivo para la realización del presente trabajo ya que consta como inventario anteriormente adquirido, pero se lo considera dentro del presupuesto general debido al uso y desgaste que sufrirá en el desarrollo del mismo.

Elaborado por: P.A.M.G	**Fecha:** 2019-12-01
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-01

3.3.1.7. *Programas específicos*

	AUDITORÍA INFORMÁTICA **PROGRAMA DE AUDITORÍA** **SEGURIDAD LÓGICA** **ARCHIVO CORRIENTE**	**PASL 1/4**

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

I. Objetivos	**REALIZADO**	**DESARROLLADO**	**FECHA**
▪ Comprobar si el software utilizado en la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo cumple con todas las especificaciones necesarias tanto: técnicas, legales, sociales y satisfacen los requerimientos a los cuales son destinados.			
II. Procedimientos			
1. Dentro del Software utilizado deberá comprobar:			
a) Que existan un control de modificaciones al sistema operativo.		**P.A.M.G**	Nov 10
b) Que se evite realizar cambios no autorizados.		**P.A.M.G**	Nov 10
c) Que se revise los procedimientos de obtención de backup.		**P.A.M.G**	Nov 10
d) Que disponga la Metodología de selección de paquetes de software.		**P.A.M.G**	Nov 10
e) Que tenga a disposición y actualizadas el estado de las licencias necesarias.		**P.A.M.G**	Nov 10
2. Dentro de la base de datos de la Empresa verificar:			
a) Que se encuentre integro la base de datos.		**P.A.M.G**	Nov 10
b) Que contengan documentación necesaria de la Base de Datos.		**P.A.M.G**	Nov 10
c) Que se asegure la existencia de backup.		**P.A.M.G**	Nov 10
d) Que esté actualizado el estado de las licencias.		**P.A.M.G**	Nov 10

Elaborado por: P.A.M.G	**Fecha:** 2019-12-01
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-01

	AUDITORÍA INFORMÁTICA PROGRAMA DE AUDITORÍA SEGURIDAD LÓGICA ARCHIVO CORRIENTE	PASL 2/4

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

	REALIZADO	DESARROLLADO	FECHA
3. Dentro del Sistema de Redes:			
a) Que existe la debida seguridad y es compatible el Sistema.	☐	P.A.M.G	Nov 12
b) Que existe un control adecuado en el acceso a datos en red.	☐	P.A.M.G	Nov 12
c) Que cuenta con un software de comunicación y sistema operativo de red – control de rendimiento de la red.	☐	P.A.M.G	Nov 12
d) Que abastece de información a todo el personal.	☐	P.A.M.G	Nov 12
e) Que cuenta con planes de infraestructura de red.	☐	P.A.M.G	Nov 12
f) Que cuenta con estándares y políticas para el control de la red.	☐	P.A.M.G	Nov 12
g) Que cuenta con el control del hardware y el software necesario	☐	P.A.M.G	Nov 12
4. Dentro de los sistemas locales y online comprobar:			
a) Que se mantenga actualizado el software.	☐	P.A.M.G	Nov 12
b) Que se revisen los procedimientos de entrada de datos online.	☐	P.A.M.G	Nov 12
c) Que se mantenga actualizado los datos online.	☐	P.A.M.G	Nov 12
d) Que el usuario tenga acceso directo al sistema y lo controla a través de terminales del software utilizados.	☐	P.A.M.G	Nov 12
e) Que exista sistemas de consultas.	☐	P.A.M.G	Nov 12

Elaborado por: P.A.M.G	**Fecha:** 2019-12-01
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-01

	AUDITORÍA INFORMÁTICA PROGRAMA DE AUDITORÍA SEGURIDAD LÓGICA ARCHIVO CORRIENTE	PASL 3/4

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

	REALIZADO	DESARROLLADO	FECHA
5. Dentro de los Datos comprobar y examinar que ningún usuario puede acceder a datos que no le competen o restringidos:			
a) Que las claves de acceso se encuentre con las seguridades necesarias	☐	P.A.M.G	Nov 12
b) Que exista un control de acceso a los respaldos.	☐	P.A.M.G	Nov 12
c) Que exista un seguimiento en las actividades del usuario.	☐	P.A.M.G	Nov 12
d) Que exista una encriptación de datos.	☐	P.A.M.G	Nov 12
e) Que los passwords se encuentren con cambios periódicos.	☐	P.A.M.G	Nov 12
f) Que los perfiles de tengan un acceso restringido a sus datos.	☐	P.A.M.G	Nov 12
g) Que exista un Bloque en las Terminales en el acceso erróneo	☐	P.A.M.G	Nov 12
6. Dentro de la actualización online revisar:			
a) Que se encuentre automatizado.	☐	P.A.M.G	Nov 12
b) Que prevén oportunamente la corrección de errores y su impacto.	☐	P.A.M.G	Nov 12
c) Que se revise los archivos que se hayan modificado.	☐	P.A.M.G	Nov 12
d) Que exista los controles de acceso necesarios al sistema.	☐	P.A.M.G	Nov 12
e) Que se revise que existan puntos de control en el acceso.	☐	P.A.M.G	Nov 12
f) Que se realizan revisiones en los registros actualizados.	☐	P.A.M.G	Nov 12

Elaborado por: P.A.M.G	**Fecha:** 2019-12-01
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-01

	AUDITORÍA INFORMÁTICA PROGRAMA DE AUDITORÍA SEGURIDAD LÓGICA ARCHIVO CORRIENTE	PASL 4/4

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

	REALIZADO	DESARROLLADO	FECHA
7. Dentro del análisis de la seguridad			
a) Que usan protocolos de red seguros para transferencia de datos.	☐	P.A.M.G	Nov 12
b) Que dispongan de medidas de seguridad para su acceso.	☐	P.A.M.G	Nov 12
c) Que disponga de seguridad de programas, archivos, backup, etc.	☐	P.A.M.G	Nov 12
d) Que la disponibilidad de equipos alternativos cubran las necesidades mínimas.	☐	P.A.M.G	Nov 12
e) Que disponga de planes de contingencias.	☐	P.A.M.G	Nov 12

Elaborado por: P.A.M.G	**Fecha:** 2019-12-01
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-01

	AUDITORÍA INFORMÁTICA PROGRAMA DE AUDITORÍA SEGURIDAD FÍSICA ARCHIVO CORRIENTE	PASF 1/2

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

I. Objetivos	REALIZADO	DESARROLLADO	FECHA
▪ Evidenciar el estado de la seguridad, calidad y uso eficiente de los equipos de escritorio, equipos servidores, infraestructura de red y de los periféricos se encuentran en buenas condiciones para su utilización. ▪ Comprobar si existen medidas de contingencias ante cualquier desastre, y combatirlo a través de medios de emergencia hasta que sea restaurado el servicio completo.			
II. Procedimientos			
1. Dentro del sistema central de los servidores, provea la siguiente información: a) Marca, modelo b) Sistema Operativo, versión c) Ubicación	□	**P.A.M.G**	Nov 13
2. Dentro del mantenimiento conocer cómo se encuentran los ordenadores	□□	**P.A.M.G**	Nov 13
3. Dentro de los Sistemas Documentales revisar su archivo adecuado.	□	**P.A.M.G**	Nov 13
4. Dentro del hardware conocer si existe el control y registro de las adquisiciones, o cambios.	□	**P.A.M.G**	Nov 13

Elaborado por: P.A.M.G	**Fecha:** 2019-12-01
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-01

	AUDITORÍA INFORMÁTICA PROGRAMA DE AUDITORÍA SEGURIDAD FÍSICA ARCHIVO CORRIENTE	PASF 2/2

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

	REALIZADO	DESARROLLADO	FECHA
5. Dentro de las Instalaciones revisar que las entradas del aire se encuentran bien para su uso, los accesos se encuentra restringidos, los circuitos de vigilancia, registro de ingreso y egreso, respaldos en medios físicos verificar:			
a) Que exista las seguridades suficientes como seguros, vigilancia, etc.	□	P.A.M.G	Nov 13
b) Que en las instalaciones contenga una fuente de poder interrumpible, tanto en los ordenadores como en la red y demás periféricos.	□	P.A.M.G	Nov 13
c) Que revise el número de extintores, su capacidad, fácil acceso, y tipo de producto que utilizan.	□	P.A.M.G	Nov 13
d) Que investigue si el personal sabe usar los equipos contra incendio y si ha habido prácticas en cuanto a su uso.	□	P.A.M.G	Nov 13
e) Que verifique si existen suficientes salidas de emergencia y que estén debidamente controladas para evitar robos por medio de estas salidas.	□	P.A.M.G	Nov 13

Elaborado por: P.A.M.G	**Fecha:** 2019-12-01
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-01

	AUDITORÍA INFORMÁTICA PROGRAMA DE AUDITORÍA TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN ARCHIVO CORRIENTE	PATC 1/4

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

I. Objetivos	REALIZADO	DESARROLLADO	FECHA
▪ Verificar el estado actual de los medios de seguridad disponibles en los equipos, a través de las restricciones a programas, archivos y usuarios. ▪ Comprobar como el sistema de información beneficia al proceso administrativo el cual es planear, organizar y controlar, con esto reducir la duplicidad de datos, de reportes y aumentar el nivel de seguridad.			
II. Procedimientos	□		
1. Dentro de las medidas de seguridad revisar: a) Revisar el estado de registro de los accesos a la información confidencial.		**P.A.M.G**	Nov 13
b) Desarrollar periódicamente una constatación física en el uso de información y de los reportes obtenidos.	□	**P.A.M.G**	Nov 13
c) Asegurar que los datos y archivos usados sean los adecuados, evitando la reproducción de datos de manera indebida.	□	**P.A.M.G**	Nov 13
d) Restringir la entrada a la red a personas no autorizadas.	□	**P.A.M.G**	Nov 13
e) Investigar el estado de restricción dentro del acceso a sistemas informáticos, a los programas y a los archivos.	□	**P.A.M.G**	Nov 13
f) Que la supervisión a los trabajadores se encuentren en estado restrictivo evitando modificar los programas.	□	**P.A.M.G**	Nov 13

Elaborado por: P.A.M.G	**Fecha:** 2019-12-01
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-01

	AUDITORÍA INFORMÁTICA PROGRAMA DE AUDITORÍA TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN ARCHIVO CORRIENTE	PATC 2/4

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

	REALIZADO	DESARROLLADO	FECHA
2. Dentro de los datos recolectados verificar que sean registrados de manera completa revisando:			
a) Realizar un estricto control sobre el acceso físico a los archivos.	☐	P.A.M.G	Nov 13
b) Supervisar la entrega de los informes, reportes, memorándums, entre otros.	☐	P.A.M.G	Nov 13
c) Realizar respaldos de los archivos y programas en lugares ajenos al centro de cómputo y en las instalaciones de alta seguridad.	☐	P.A.M.G	Nov 13
3. Dentro del manejo de la Información y su seguridad revisar:			
a) Realizar periódicamente el control de las bitácoras tanto de los procesos adecuados e inadecuados.	☐	P.A.M.G	Nov 13
b) Realizar y controle de manera periódica la distribución y destrucción de todos los datos o reportes confidenciales	☐	P.A.M.G	Nov 13
c) Realizar copias indebidas y sin autorización de archivos restringidos.	☐	P.A.M.G	Nov 13
d) Revisar que personal no autorizado ingrese a Información de carácter confidencial.	☐	P.A.M.G	Nov 13

Elaborado por: P.A.M.G	**Fecha:** 2019-12-01
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-01

	AUDITORÍA INFORMÁTICA PROGRAMA DE AUDITORÍA TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN ARCHIVO CORRIENTE	PATC 3/4

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

	REALIZADO	DESARROLLADO	FECHA
4. Dentro de la seguridad en la información conocer si la Institución cuenta con respaldos de los sistemas, programas, archivos y la documentación necesarios verificar:			
a) Cumplir con los requerimientos físicos.	☐	P.A.M.G	Nov 13
b) Revisar cada ordenador con Equipos, programas y archivos	☐	P.A.M.G	Nov 13
c) Revisar que cuente con un control de aplicaciones por ordenador	☐	P.A.M.G	Nov 13
d) Disposición de estrategias de seguridad de la red y de respaldos	☐	P.A.M.G	Nov 13
5. Dentro de los sistemas se encuentran interrelacionados y no son programas que funcionen por separado.	☐	P.A.M.G	Nov 13
6. Dentro del nivel de seguridad, sólo las personas autorizadas tienen acceso y no genere duplicidad en la información.	☐	P.A.M.G	Nov 13
7. Dentro de los Sistemas Informáticos verifique:			
a) Los equipos sean modernos	☐	P.A.M.G	Nov 13
b) Los equipos se encuentren de manera eficientes	☐	P.A.M.G	Nov 13
c) Disposición de herramientas para la toma de decisiones.	☐	P.A.M.G	Nov 13
d) Ser necesarios para el trabajo de cada trabajador.	☐	P.A.M.G	Nov 13
e) Sean de fácil uso y comprensibles para el usuario.	☐	P.A.M.G	Nov 13
f) Sean eficaces en el momento de su uso.	☐	P.A.M.G	Nov 13
g) Presten la información adecuada y necesaria a cada servidor.	☐	P.A.M.G	Nov 13
h) La información sea la misma tanto a nivel Directivo y el nivel Operativo	☐	P.A.M.G	Nov 13

Elaborado por: P.A.M.G	**Fecha:** 2019-12-01
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-01

	AUDITORÍA INFORMÁTICA PROGRAMA DE AUDITORÍA TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN ARCHIVO CORRIENTE	PATC 4/4

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

	REALIZADO	DESARROLLADO	FECHA
8. Dentro de la renovación y mantenimiento de recursos y archivos revisar:			
a) Encontrarse de manera constante para los recursos disponibles, tanto de equipo, sistemas y comunicaciones.	☐	**P.A.M.G**	Nov 13
b) Los documentos de manera permanente y registros para renovarlos o tenerlos actualizados.	☐	**P.A.M.G**	Nov 13
9. Dentro se seguridad física se tiene equipos los cuales permitan seguir operando en caso de falta de la corriente eléctrica, vías alternas de comunicación y equipo alternativo para las operaciones.	☐	**P.A.M.G**	Nov 13

Elaborado por: P.A.M.G	**Fecha:** 2019-12-01
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-01

	AUDITORÍA INFORMÁTICA PROGRAMA DE AUDITORÍA GESTIÓN INFORMÁTICA ARCHIVO CORRIENTE	**PAGI 1/3**

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

	REALIZADO	DESARROLLADO	FECHA
I. Objetivos			
▪ Asegurar la gestión la cual debe mantenerse de una manera adecuada en la utilización de los recursos informáticos de la institución.	☐	**P.A.M.G**	Nov 14
II. Procedimientos			
1. Dentro de los usuarios responsables de mantener y modificar la información se encuentran bien definidos en sus labores y poseen accesos únicos y restringidos de acuerdo a niveles.	☐	**P.A.M.G**	Nov 14
2. Dentro de la seguridad en la red, revisar si no existe plagio, fuga de información y posible adquisición o traspaso de virus.	☐	**P.A.M.G**	Nov 13
3. Dentro del uso de los ordenadores revisar:			
a) Que no exista ningún tipo de uso ajeno a las actividades normales de la institución.	☐	**P.A.M.G**	Nov 13
b) Que evite el plagio de los programas utilizados por la empresa ya que cae en delito por Derechos de Autor.	☐	**P.A.M.G**	Nov 13
c) Que el acceso a bases de datos sea exclusiva a fin de evitar modificaciones de la información con propósitos fraudulentos.	☐	**P.A.M.G**	Nov 13
4. Dentro de seguridad lógica revisar la existencia de un método eficaz para proteger sistemas de computación a través de un software de control de acceso.	☐	**P.A.M.G**	Nov 13

Elaborado por: P.A.M.G	**Fecha:** 2019-12-01
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-01

	AUDITORÍA INFORMÁTICA PROGRAMA DE AUDITORÍA GESTIÓN INFORMÁTICA ARCHIVO CORRIENTE	PAGI 2/3

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

	REALIZADO	DESARROLLADO	FECHA
5. Dentro del sistema integral de seguridad verificar:			
a) Que prácticas de seguridad del personal se aplica	☐	P.A.M.G	Nov 13
b) Que medios de seguridad física y contra catástrofes posee la Institución.	☐	P.A.M.G	Nov 13
c) Que elementos administrativos tiene la institución	☐	P.A.M.G	Nov 13
d) Que definición de políticas de seguridad aplica.	☐	P.A.M.G	Nov 13
e) Que sistemas de seguridad se aplican dentro de los elementos técnicos y operativos	☐	P.A.M.G	Nov 13
f) Que se revise el Sistemas de seguridad tanto en servidores y terminales de la institución.	☐	P.A.M.G	Nov 13
g) Que se verifique la cadena de mando y responsabilidades.	☐	P.A.M.G	Nov 13
h) Que se revisen los datos y archivos que se generan en la institución	☐	P.A.M.G	Nov 13
6. Dentro del riesgo y su clasificación verificar:			
a) Que se revise los datos, la información y programas con datos confidenciales para la empresa y también información con Datos relevantes de la empresa.	☐	P.A.M.G	Nov 13
b) Que se compruebe la información que tenga un gran costo financiero o un gran impacto en la toma de decisiones.	☐	P.A.M.G	Nov 13

Elaborado por: P.A.M.G	**Fecha:** 2019-12-01
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-01

	AUDITORÍA INFORMÁTICA **PROGRAMA DE AUDITORÍA** **GESTIÓN INFORMÁTICA** **ARCHIVO CORRIENTE**	**PAGI 3/3**

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

	REALIZADO	DESARROLLADO	FECHA
7. Dentro de las precauciones del riesgo que tenga la información con respecto al tipo y tamaño de la organización verificar.			
a) Que el personal que prepara la información debe tener acceso a la operación.	□	**P.A.M.G**	Nov 13
b) Que los operadores dispongan de acceso a los archivos almacenados.	□	**P.A.M.G**	Nov 13
c) Que los operadores deben ser los únicos que tengan el control sobre los trabajos procesados y debe existir correcciones a los errores detectados.	□	**P.A.M.G**	Nov 13

Elaborado por: P.A.M.G	**Fecha:** 2019-12-01
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-01

3.3.1.8. *Selección de métodos, técnicas e instrumentos*

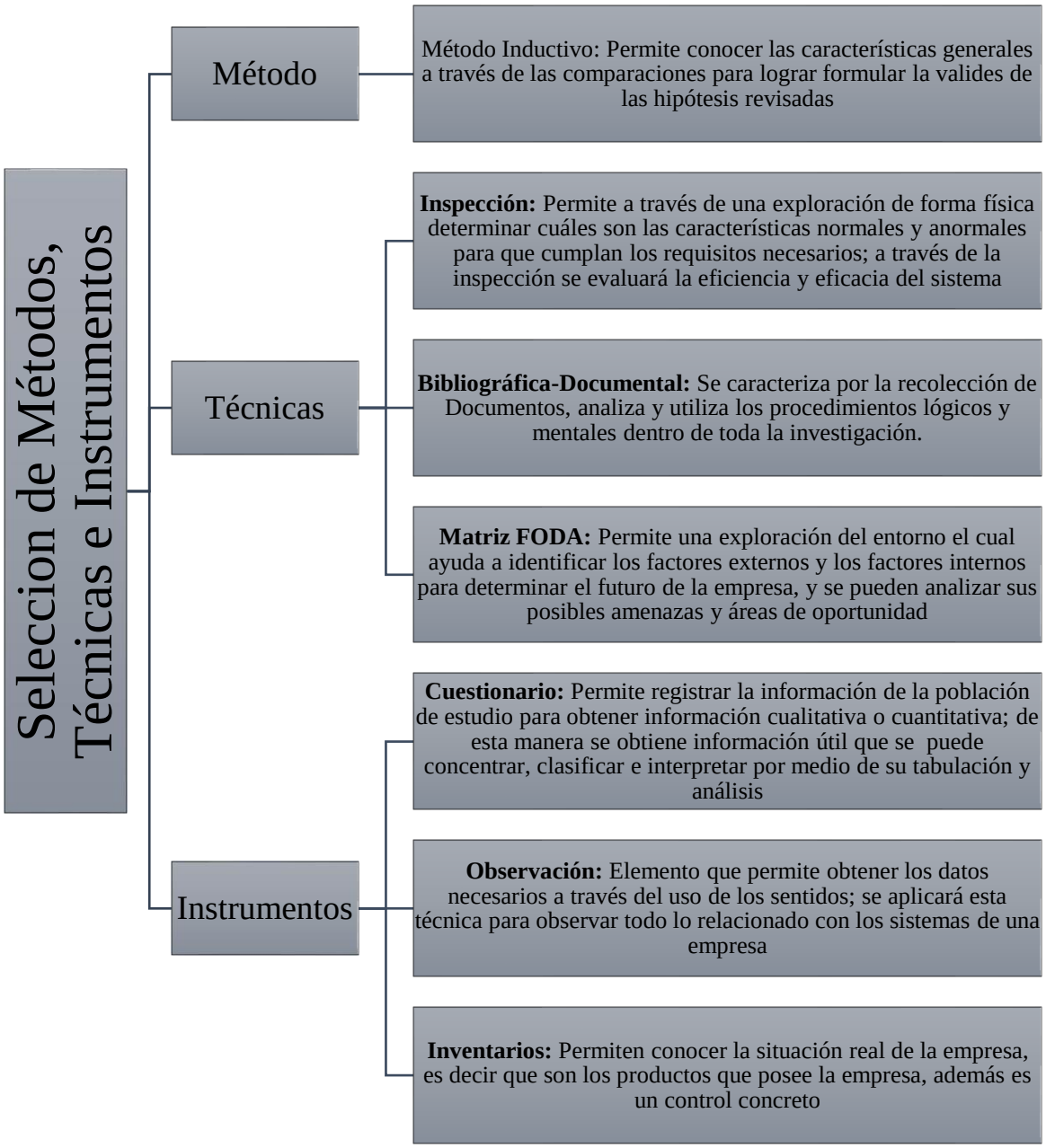


Figura 12-4: Selección de Métodos, Técnicas e Instrumentos

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

FASE II: Ejecución de la Auditoría

3.3.2. *Ejecución de la auditoría*

3.3.2.1. *Cuestionario de control interno específicos aplicando el COSO 2*

	AUDITORÍA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO SEGURIDAD LÓGICA ARCHIVO CORRIENTE	CCISL 1/3

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática **Componente:** Seguridad lógica
Período: Año 2018

CUESTIONARIO	SI	NO	N/A	OBSERVASIONES
Ambiente Interno				
1. ¿Se adquiere las licencias necesarias para el uso de todos los Programas disponibles en la Organización?	✓			
2. ¿La empresa posee un antivirus para evitar posibles fallos en el sistema?	✓			
3. ¿La Organización posee un Cortafuegos debidamente Configurado el cual evite accesos de terceros?	✓			
4. ¿La Contraseña posee un número mínimo de caracteres?	✓			
5. ¿Cuándo finaliza los Labores de un empleado, se da de baja su acceso?	✓			
Establecimiento de Objetivos				
6. ¿Los programas se encuentran actualizados?	✓			**Cada vez que existe un parche de actualización**
7. ¿Los programas para detección se mantienen actualizados?	✓			**De forma automática**
Identificación de Eventos				
8. ¿Existen un registro o logs que permitan conocer si existen accesos no autorizados?	✓			
9. ¿Los Usuarios solo tienen disponible los módulos para su labor?	✓			**Solo se activan los módulos necesarios para el desempeño de los labores**
Evaluación de Riesgos				
10. ¿Revisa de manera regular los programas instalados?		✓		**Cuando existe algún fallo realizan la revisión**
11. ¿El nivel de Seguridad en las Contraseñas constan: números, letras, signos de puntuación, caracteres especiales?	✓			**A excepción los signos de puntuación**

Elaborado por: P.A.M.G	**Fecha:** 2019-12-05
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-05

	AUDITORÍA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO SEGURIDAD LÓGICA ARCHIVO CORRIENTE	CCISL 2/3

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática **Componente:** Seguridad lógica
Período: Año 2018

CUESTIONARIO	SI	NO	N/A	OBSERVASIONES.
Respuesta al Riesgo				
12. ¿Se tiene previsto en el plan de contingencias, como actuar si existe modificaciones de claves no previstas?		✓		**Dentro del Plan de Contingencias no existe esta previsión.**
13. ¿Se modifica de manera constante las Claves de acceso?	✓			**El Sistema lo solicita cada 30 Días**
Actividades de Control				
14. ¿Poseen los equipos medios de seguridad tales como: claves de acceso?	✓			
15. ¿Realiza un seguimiento de las Operaciones?	✓			**Tres veces a la Semana**
16. ¿Existe limitantes de acceso en los Intentos Fallidos?	✓			**3 veces lo permite el Sistema**
Información y Comunicación				
17. ¿Se tiene un Control para la revisión de los mecanismos de seguridad?	✓			**El control se lo realiza una vez a la semana**
18. ¿Cada Usuario se Identifica su acceso?	✓			
Monitoreo				
19. ¿En alguna ocasión en el periodo auditado se ha encontrado algún programa malicioso?		✓		
20. ¿En los Ficheros se almacena Datos de Carácter Personal de los Usuarios?		✓		**Los ficheros no permiten el almacenamiento de estos Datos**
TOTAL	**16**	**4**	**0**	
RESPUESTAS POSITIVAS	**16**	≡	**75,0 %**	
RESPUESTAS NEGATIVAS	**4**	≡	**25,00 %**	

Elaborado por: P.A.M.G **Fecha:** 2019-12-05
Revisado por: W.G.Y.C H.B.V.S **Fecha:** 2019-12-05

	AUDITORÍA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO INTERNO SEGURIDAD LÓGICA ARCHIVO CORRIENTE	CCISL 3/3

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática **Componente:** Seguridad lógica
Período: Año 2018

MEDICIÓN DE NIVELES DE RIESGO Y CONFIANZA[12]

Tabla 12-4: Nivel de Riesgo y Confianza Seguridad Lógica

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

Fuente: Desarrollo de la Investigación
Realizado por: Paúl Alejandro Merizalde Guamanzara

Análisis.-.

Después de la ejecución del cuestionario de control interno seguridad lógica se constató que el existe un Nivel de Riesgo BAJO que corresponde al 25,00 %, las cuales son las respuestas negativas e indica que la realización de la Auditoría se realizara sin ningún tipo de Riesgo; por otro lado el Nivel de Confianza es ALTO el cual corresponde al 75,00 %, que son las respuestas positivas lo que indica que el Auditor no se compromete bajo ningún termino en los resultados de la Auditoria

Elaborado por: P.A.M.G	**Fecha:** 2019-12-05
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-05

[12] **Nota:** Análisis del Nivel de Riesgo y Confianza del Control Interno de la Seguridad Lógica

	AUDITORÍA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO SEGURIDAD FÍSICA ARCHIVO CORRIENTE	CCISF 1/5

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática **Componente:** Seguridad física
Período: Año 2018

CUESTIONARIO	SI	NO	N/A	OBSERVASIONES.
Ambiente Interno				
1. ¿La organización cuenta con copias o respaldos físicos?	✓			**Se encuentran en la bóveda de la Organización y en una Caja de Seguridad en el Banco del Austro.**
2. ¿El centro de cómputo se encuentra conectada al exterior?	✓			
3. ¿La Seguridad es Contratada?	✓			**Para la seguridad se establece un Contrato de servicios profesionales**
4. ¿La Organización cuenta con salida de Emergencia?	✓			
5. ¿El cableado de la Red se encuentra debidamente instalado?	✓			
Establecimiento de Objetivos				
6. ¿En el Departamento de Sistemas existe prohibición de consumo de alimentos y bebidas para evitar los posibles daños y averías?	✓			
7. ¿No existen obstáculos, se encuentran al alcance y están debidamente etiquetados los interruptores de Luz?	✓			
8. ¿Posee una clasificación de la Información, y como se la clasifica dentro de la Organización?	✓			**a) Vital: Base de datos, instaladores, claves, reportes** **b) Esencial: Información**

Elaborado por: P.A.M.G	**Fecha:** 2019-12-05
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-05

	AUDITORÍA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO SEGURIDAD FÍSICA ARCHIVO CORRIENTE	CCISF 2/5

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática **Componente:** Seguridad física
Período: Año 2018

CUESTIONARIO	SI	NO	N/A	OBSERVASIONES.
Identificación de Eventos				
9. ¿Las Instalaciones donde se encuentra todo el equipo para el funcionamiento Informático de la Organización se encuentra seguro?	✓			**Es adecuado el lugar**
10. ¿Existe personal responsable de la Seguridad de la Organización?	✓			
11. La salida de Emergencia puede abrirse por ambos lados:		✓		**Solo se abre desde adentro**
12. ¿Existen medidas para evitar incendios en la Organización?	✓			**Los empleados tienen prohibido fumar en las Instalaciones, evita la utilización de productos inflamables y se monitorea las conexiones eléctricas**
13. ¿En cuanto a las operaciones, se encuentran interconectadas las Terminales?	✓			
Evaluación de Riesgos				
14. ¿Las instalaciones son adecuadas para el centro de Cómputo y cómo se encuentran?	✓			**Los espacios para el trabajo se encuentran remodeladas**
15. Los extintores son en base de:			✓	**Polvo/ Espuma**
16. ¿El material emitido por los extinguidores con su uso no hace más daño que el mismo incendio?	✓			
17. ¿Los Servidores en la Organización se encuentran debidamente protegidos?	✓			

Elaborado por: P.A.M.G **Fecha:** 2019-12-05
Revisado por: W.G.Y.C H.B.V.S **Fecha:** 2019-12-05

	AUDITORÍA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO SEGURIDAD FÍSICA ARCHIVO CORRIENTE	CCISF 3/5

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática **Componente:** Seguridad física
Período: Año 2018

CUESTIONARIO	SI	NO	N/A	OBSERVASIONES.
Respuesta al Riesgo				
18. ¿Se realizan copias o respaldos en lugares distintos de la Computadora?	✓			
19. ¿Existen alarmas dentro de la Organización? ¿Cuáles son estas?	✓			**Las alarmas que posee son: Contra Fuego, Contra Robo, Alarma en la Entrada**
20. ¿En la Organización cuentan con extintores?	✓			**Manuales**
21. ¿El personal de la organización sabe cómo manipular los extintores en casos trágicos?	✓			
22. ¿La Organización cuenta con Reguladores de voltaje los cuales evitan subidas o bajadas eléctricas?	✓			
Actividades de Control				
23. ¿Existe seguridad en la entrada al laboratorio de cómputo y cuál es?	✓			**Se ingresa a través de las llaves entregadas al Personal de Sistemas de la Organización**
24. ¿Posee alarmas la organización y dónde se encuentran ubicadas?	✓			**Contra Fuego: En el espacio de los Clientes y en lugar exclusivo de los empleados Contra Robo: en los cajeros, Alarma en la Entrada: en la puerta secundaria la cual se conecta con la a Empresa de vigilancia**

Elaborado por: P.A.M.G	**Fecha:** 2019-12-05
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-05

	AUDITORÍA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO SEGURIDAD FÍSICA ARCHIVO CORRIENTE	CCISF 4/5

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática **Componente:** Seguridad física
Período: Año 2018

CUESTIONARIO	SI	NO	N/A	OBSERVASIONES.
25. ¿Si existiera un incendio, saben los operadores de Sistemas el correcto proceder?		✓		**La empresa cuenta con manual de contingencias pero no se ha comunicado**
26. ¿Los extintores se encuentran en constante monitoreo por su proveedor?	✓			**El Cuerpo de Bomberos los monitorea**
27. ¿Se realiza una identificación de los Usuarios?		✓		**La identificación de los Usuarios se las realiza pocas veces**
Información y Comunicación				
28. ¿Se Registra el Acceso al Departamento de Sistemas de parte de personas ajenas al Departamento?		✓		**Existe bitácora de registro pero pocas veces se lo registra**
29. ¿Las alarmas son audibles?	✓			
Monitoreo				
30. ¿El Departamento posee medidas de Seguridad?	✓			**Cámaras de Vigilancia y registros escritos de entrada y salida de personal**
31. ¿La salida de Emergencia se encuentra en constante monitoreo para evitar posibles catástrofes?	✓			**El Conserje se encarga del mantenimiento**
TOTAL	**26**	**4**	**1**	
RESPUESTAS POSITIVAS	**26**	**≡**	**83,87 %**	
RESPUESTAS NEGATIVAS	**4**	**≡**	**12,90 %**	
RESPUESTAS NO APLICAN	**1**	**≡**	**3,23 %**	

Elaborado por: P.A.M.G **Fecha:** 2019-12-05
Revisado por: W.G.Y.C H.B.V.S **Fecha:** 2019-12-05

	AUDITORÍA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO SEGURIDAD FÍSICA ARCHIVO CORRIENTE	CCISF 5/5

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática **Componente:** Seguridad física
Período: Año 2018

MEDICIÓN DE NIVELES DE RIESGO Y CONFIANZA[13]

Tabla 13-4: Nivel de Riesgo y Confianza Seguridad Física

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

Fuente: Desarrollo de la Investigación
Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Análisis.-.

Después de la ejecución del cuestionario de control interno seguridad física se constató que el existe un Nivel de Riesgo BAJO que corresponde al 16,13 %, las cuales son las respuestas negativas y las respuestas que no aplican el cual indica que la realización de la Auditoría se realizara sin ningún tipo de Riesgo; por otro lado el Nivel de Confianza es ALTO el cual corresponde al 83,87 %, que son las respuestas positivas lo que indica que el Auditor no se compromete bajo ningún termino en los resultados de la Auditoria

Elaborado por: P.A.M.G	**Fecha:** 2019-12-05
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-05

[13] Análisis del Nivel de Riesgo y Confianza del Control Interno de la Seguridad Física

	AUDITORÍA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO TECNOLOGÍAS DE LA IFORMACIÓN Y COMUNICACIÓN ARCHIVO CORRIENTE	CCITIC 1/2

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática **Componente:** Tic
Período: Año 2018

CUESTIONARIO	SI	NO	N/A	OBSERVASIONES.
Ambiente Interno				
1. ¿La organización utiliza Internet?	✓			
2. ¿La organización utiliza la Intranet?		✓		
Establecimiento de Objetivos				
3. ¿La Organización cuenta con página Web?	✓			
Identificación de Eventos				
4. ¿Para la comunicación entre empleados, lo realiza a través del Correo Electrónico y cuáles son sus características?	✓			**Que es Genérico y además es Personalizado**
Evaluación de Riesgos				
5. ¿La Velocidad de Internet es buena para las labores de la organización y como se encuentra distribuida?		✓		**2 Mb de bajada 1 Mb de subida**
6. ¿Cuenta con distribución de Internet y como se encuentra?	✓			**A través de la conexión cableada a todas las terminales y por medio de WI- FI para el backup.**
Respuesta al Riesgo				
7. ¿Si existiese algún fallo o daño en el servicio de Internet, el proveedor lo soluciona ágilmente?	✓			
Actividades de Control				
8. ¿Los correos electrónicos de los socios se encuentran enlistados e ingresados?	✓			
Información y Comunicación				
9. ¿La organización cuenta con un proveedor de internet y se llama?	✓			**Telconet / Puntonet**
10. ¿Se utiliza tecnología VOIP para la comunicación?		✓		**Usa los medios Tradicionales**
Monitoreo				
11. ¿Se encuentra actualizada la Pagina Web?	✓			
12. ¿La Página Web permite a los socios brindarles servicios?	✓			
TOTAL	**9**	**3**	**0**	
RESPUESTAS POSITIVAS	**9**	≡	**75,00 %**	
RESPUESTAS NEGATIVAS	**3**	≡	**25,00 %**	
RESPUESTAS NO APLICAN	**0**	≡	**00,00 %**	

Elaborado por: P.A.M.G	**Fecha:** 2019-12-05
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-05

	AUDITORÍA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN ARCHIVO CORRIENTE	CCITIC 2/2

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática **Componente:** Tic
Período: Año 2018

MEDICIÓN DE NIVELES DE RIESGO Y CONFIANZA[14]

Tabla 14-4: Nivel de Riesgo y Confianza Tecnologías de la Información y Comunicación

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

Fuente: Desarrollo de la Investigación
Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Análisis.-.

Después de la ejecución del cuestionario de control interno tecnologías de la información y comunicación se constató que el existe un Nivel de Riesgo BAJO que corresponde al 25,00 %, las cuales son las respuestas negativas y las respuestas que no aplican el cual indica que la realización de la Auditoría se realizara sin ningún tipo de Riesgo; por otro lado el Nivel de Confianza es ALTO el cual corresponde al 75,00 %, que son las respuestas positivas lo que indica que el Auditor no se compromete bajo ningún termino en los resultados de la Auditoria

Elaborado por: P.A.M.G	**Fecha:** 2019-12-05
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-05

[14]**Nota:** Análisis del Nivel de Riesgo y Confianza del Control Interno de las Tecnologías de la Información y Comunicación

	AUDITORÍA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO GESTIÓN INFORMÁTICA ARCHIVO CORRIENTE	CCIGI 1/4

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática **Componente:** Gestión informática
Período: Año 2018

CUESTIONARIO	SI	NO	N/A	OBSERVASIONES.
Ambiente Interno				
1. ¿Para la identificación de puestos clave se encuentran debidamente definidas las funciones?	✓			
2. ¿La organización cuenta con un Sistema el cual permita la recolección de Datos?	✓			
3. ¿Dentro del manual existen los Procedimientos adecuados con las explicaciones correspondientes?	✓			**Todos los procesos cuentan con explicación**
4. ¿Cuenta con Políticas de Seguridad en la Organización?	✓			
Establecimiento de Objetivos				
5. ¿La Organización cuenta con procedimientos Formales los que permita una correcta operación?	✓			
6. ¿Las Políticas de Seguridad se encuentran alineadas a las Políticas de la Organización?	✓			
7. ¿Las Políticas de Seguridad se encuentran alineadas a las Políticas Legales?	✓			
8. ¿Las Políticas de Seguridad se encuentran en un lenguaje el cual sea entendido por todos los empleados de la Organización?	✓			
Identificación de Eventos				
9. ¿Posee la debida actualización de los procedimientos?	✓			**Cuando se presente alguna Actualización de equipos**
10. ¿Existe algún mecanismo para la ejecución de programas no autorizados?	✓			**El antivirus evita ejecutarlos**
11. ¿Tiene disponible algún Tipo de Seguro en el equipo?, ¿Cómo se Llama?		✓		**Empresa por contratar, Latina Seguros, un año de vigencia**

Elaborado por: P.A.M.G	**Fecha:** 2019-12-05
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-05

	AUDITORÍA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO GESTIÓN INFORMÁTICA ARCHIVO CORRIENTE	CCIGI 2/4

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática **Componente:** Gestión informática
Período: Año 2018

CUESTIONARIO	SI	NO	N/A	OBSERVASIONES.
Evaluación de Riesgos				
12. ¿En el Caso de que el Sistema Falle, dentro del manual se encuentra el procedimiento para contrarrestarlo?		✓		
13. ¿Dentro del registro se muestra el tiempo de congelación de las operaciones, si es mantenimiento o instalación de software?	✓			
14. ¿Las Políticas de Seguridad son aplicadas por todos los empleados?		✓		
Respuesta al Riesgo				
15. ¿Existe un control preventivo para evitar errores y cómo se procede?		✓		**Se revisa solo cuando existe el error después se realiza búsqueda y detección de y se procede a la realización de Documentos si fuere necesario**
16. ¿Cundo existe alguna interrupción en el Sistema, se cuenta con procedimientos escritos para su operación?		✓		**Dentro del manual de procedimientos no se encuentra**
17. ¿Se realiza intervenciones oportunas en los equipos?	✓			**Cuando sea necesario**
18. ¿Dispone de alguna Bitácora la que permite llevar el registro del sistema o equipo de cómputo?	✓			
19. ¿Cuándo la Información almacenada se considera inservible, que procede?	✓			**Se la destruye**
Actividades de Control				
20. ¿En los procesos que se genera en el computador existe un control el cual justifique su operación?	✓			**Los procesos se encuentran dentro del manual correspondiente**

Elaborado por: P.A.M.G	**Fecha:** 2019-12-05
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-05

	AUDITORÍA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO GESTIÓN INFORMÁTICA ARCHIVO CORRIENTE	CCIGI 3/4

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática **Componente:** Gestión informática
Período: Año 2018

CUESTIONARIO	SI	NO	N/A	OBSERVASIONES.
21. ¿Realizan revisiones periódicas a los sistemas para determinar si cumplen con los objetivos para los cuales fueron instalados?	✓			
22. ¿Cuenta con algún control para la realización de las actividades?	✓			**Por medio de la Utilización de Bitácoras**
23. ¿Tiene un Control por el trabajo realizado fuera del Horario establecido en la Organización?	✓			
24. ¿Se realiza la comunicación de las Políticas de Seguridad?		✓		
25. ¿Existe en la empresa un responsable encargados del desarrollo, revisión y evaluación de la Política de Seguridad con la suficiente formación y experiencia?		✓		
Información y Comunicación				
26. ¿Cuentan con un mantenimiento periódico, preventivo y correctivo en equipos que lo necesiten?		✓		
27. ¿Cómo se encuentra organizado el archivo Bitácora?	✓			**Fecha, Hora, Actividad, Responsable**
28. ¿La Organización cuenta con Departamento de Auditoria Interna?	✓			
Monitoreo				
29. ¿El operador tiene prohibido la modificación de los archivos?	✓			
30. ¿Cuenta con un Inventario Actualizado el cual conste los Equipos, Terminales, y responsables?	✓			
31. ¿El Departamento de Auditoria Interna se mantiene Informada y conoce los Aspectos de Sistemas?	✓			
TOTAL	**23**	**8**	**0**	
RESPUESTAS POSITIVAS	**24**	**≡**	**74,19 %**	
RESPUESTAS NEGATIVAS	**7**	**≡**	**25,81%**	
RESPUESTAS NO APLICAN	**0**	**≡**	**00,00 %**	

Elaborado por: P.A.M.G	**Fecha:** 2019-12-05
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-05

	AUDITORÍA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO GESTIÓN INFORMÁTICA ARCHIVO CORRIENTE	CCIGI 4/4

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática **Componente:** Gestión informática
Período: Año 2018

MEDICIÓN DE NIVELES DE RIESGO Y CONFIANZA[15]

Tabla 16-4: Nivel de Riesgo y Confianza Gestión Informática

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

Fuente: Desarrollo de la Investigación
Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Análisis.-.

Después de la ejecución del cuestionario de control interno gestión informática se constató que el existe un Nivel de Riesgo BAJO que corresponde al 25,81 %, las cuales son las respuestas negativas y las respuestas que no aplican el cual indica que la realización de la Auditoría se realizara sin ningún tipo de Riesgo; por otro lado el Nivel de Confianza es ALTO el cual corresponde al 74,19 %, que son las respuestas positivas lo que indica que el Auditor no se compromete bajo ningún termino en los resultados de la Auditoria

Elaborado por: P.A.M.G	**Fecha:** 2019-12-05
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-05

[15] **Nota:** Análisis del Nivel de Riesgo y Confianza del Control Interno de la Gestión Informática

3.3.2.2. *Análisis FODA de los sistemas informáticos*

	AUDITORÍA INFORMÁTICA **ANÁLISIS FODA** **ARCHIVO CORRIENTE**	**AFODA 1/2**

	FACTORES INTERNOS	REV		FACTORES INTERNOS	REV	
	FORTALEZAS	**AUD**		**DEBILIDADES**	**AUD**	
POSITIVO	▪ El Software utilizado por la empresa se encuentra con licencia y es utilizado.	✓		▪ No cuenta con el plan para el desecho de equipos que ya han cumplido con su vida útil	*	NEGATIVO
	▪ Con los Objetivos de la COAC se encuentra direccionado el centro de cómputo.	✓		▪ El Personal de Sistemas realiza el mantenimiento solo cuando el equipo o Sistema presenta error o daño.	*	
	▪ La COAC cuenta con conexión a la Red en todo su espacio Físico.	✓		▪ No cuenta con gran disposición económica para el mejoramiento de los equipos y los sistemas lo que dificulta la Eficiencia y Eficacia de los trabajadores.	*	
	▪ Posee medidas anti-ataques y filtraciones Informáticas.					
	▪ Ambiente laboral idóneo para la realización correcta del trabajo.	✓		▪ La empresa aun no adquiere ningún seguro, pero en el transcurso del año se lo estará adquiriendo	*	
	▪ El Sistema informático que cuenta la empresa CONEXUS permite dar seguridad y el funcionamiento adecuado a sus trabajadores, además, otorga a cada empleado lo necesario para cumplir sus actividades.	✓		▪ Desactualización de los Equipos Disponibles en la Institución.	*	
	▪ El Software se encuentra direccionado a las necesidades del negocio, actualizado constantemente.	✓		▪ Las Funciones del personal de Sistemas no se encuentra bien definidas las que no permiten su ejecución de forma eficiente.	*	
	▪ Bitácoras con todas las incidencias, cambios y procedimientos.	✓				
	▪ Documentación necesaria de soporte y los procedimientos informáticos en casi la totalidad de procesos informáticos.	✓				
	▪ El Inventario se mantiene actualizado dentro del grupo de activos tecnológicos.	✓				
	▪ El personal dentro del Departamento de Sistemas se encuentra capacitado y es el adecuado ante cualquier problema o requerimiento.	✓				
	▪ El personal administrativo tiene el conocimiento adecuado para el uso de los equipos.	✓				

Figura 13-4: Análisis FODA 1.1
Fuente: Desarrollo de la Investigación
Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Elaborado por: P.A.M.G	**Fecha:** 2019-12-05
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-05

PM Auditor y Consultor	**AUDITORÍA INFORMÁTICA** **ANÁLISIS FODA** **ARCHIVO CORRIENTE**	**AFODA 2/2**

	OPORTUNIDADES	AMENAZAS	
POSITIVO	▪ La Adquisición de Nuevas Tecnologías las que permitirán la disminución de Gastos. ▪ Uso de Software Libre el que permite mejorar la reducción de Costos y Gastos. ▪ Búsqueda de Capacitación por parte de Terceros. ▪ Aumento potencial de los salarios de los Socios. ▪ En el mercado se encuentra la oferta de Tecnología de punta la que permitirá mejorar la Eficiencia y la Eficacia de la CACECH.	▪ Competencia desleal del mercado. ▪ Los precios en el mercado de Software y Hardware son muy elevados. ▪ Los Equipos Informáticos se encuentran en evolución constante. ▪ Existencia de varios programas corruptos los cuales pueden sabotear y robar información importante de la Institución. ▪ Fallos en la energía Eléctrica, o cortes de electricidad sorpresivos.	NEGATIVO
	FACTORES EXTERNOS	FACTORES EXTERNOS	

Figura 14-4: Análisis FODA 1.2
Fuente: Desarrollo de la Investigación
Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Elaborado por: P.A.M.G	**Fecha:** 2019-12-05
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-05

3.3.2.3. *Matriz de Correlación*

Tabla 17-4: Correlación FO[16]

		F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	
	FO	El Software utilizado por la empresa	Con los Objetivos de la COAC se encuentra	La COAC cuenta con conexión a la Red	Posee medidas anti-ataques y filtraciones	Ambiente laboral idóneo para la realización	El Sistema informático que cuenta la	El Software se encuentra direccionado	Bitácoras con todas las incidencias, cambios	Documentación necesaria de soporte	El Inventario se mantiene actualizado	El personal dentro del Departamento	El personal administrativo tiene el	**TOTAL**
O1	La Adquisición de Nuevas	**5**	**3**	**5**	**5**	**3**	**5**	**5**	**5**	**5**	**5**	**1**	**3**	**50**
O2	Uso de Software Libre	**5**	**1**	**5**	**5**	**3**	**1**	**5**	**3**	**5**	**5**	**1**	**3**	**42**
O3	Búsqueda de Capacitación	**3**	**3**	**5**	**1**	**5**	**3**	**3**	**1**	**3**	**1**	**5**	**5**	**38**
O4	Aumento potencial de los	**1**	**3**	**3**	**1**	**3**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**18**
O5	En el mercado se encue	**5**	**3**	**3**	**5**	**1**	**5**	**5**	**1**	**1**	**5**	**1**	**1**	**36**
	TOTAL	**19**	**13**	**21**	**17**	**15**	**15**	**19**	**11**	**15**	**17**	**9**	**13**	**184**

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Elaborado por: P.A.M.G	**Fecha:** 2019-12-05
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-05

[16] **Nota:** Matriz de Correlación FO

Tabla 18-4: Correlación DA

		D1	D2	D3	D4	D5	D6	
	DA	No cuenta con el plan para el desecho de equipos que ya han cumplido	El Personal de Sistemas realiza el mantenimiento solo cuando el equipo o Sistema	No cuenta con gran disposición económica para el mejoramiento de los equipos.	La empresa aun no adquiere ningún seguro, pero en el transcurso del año	Desactualización de los Equipos Disponibles en la Institución.	Las Funciones del personal de Sistemas no se encuentra bien definidas	TOTAL
A 1	Competencia desleal del mercado.	**1**	**1**	**1**	**1**	**3**	**1**	**8**
A 2	Los precios en el mercado de Software y	**5**	**3**	**5**	**3**	**5**	**1**	**22**
A 3	Los Equipos Informáticos se encuentran en.	**5**	**3**	**5**	**3**	**5**	**1**	**22**
A 4	Existencia de varios programas	**1**	**5**	**5**	**1**	**5**	**1**	**18**
A 5	Fallos en la energía Eléctrica, o	**1**	**5**	**5**	**1**	**5**	**1**	**18**
	TOTAL	**13**	**17**	**21**	**9**	**23**	**5**	**88**

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Elaborado por: P.A.M.G	**Fecha:** 2019-12-05
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-05

3.3.2.4. *Matriz de Prioridades*

	AUDITORÍA INFORMÁTICA MATRIZ DE PRIORIDADES ARCHIVO CORRIENTE	**MPRI 1/3**

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

MATRIZ DE PRIORIDADES

VARIABLES INTERNAS

∑	**FORTALEZAS**
F3	La COAC cuenta con conexión a la Red en todo su espacio Físico.
F1	El Software utilizado por la empresa se encuentra con licencia y es utilizado
F7	El Software se encuentra direccionado a las necesidades del negocio, actualizado constantemente
F4	Posee medidas anti-ataques y filtraciones Informáticas
F10	El Inventario se mantiene actualizado dentro del grupo de activos tecnológicos
F9	Documentación necesaria de soporte y los procedimientos informáticos en casi la totalidad de procesos informáticos
F6	El Sistema informático que cuenta la empresa CONEXUS permite dar seguridad y el funcionamiento adecuado a sus trabajadores, además, otorga a cada empleado lo necesario para cumplir sus actividades
F5	Ambiente laboral idóneo para la realización correcta del trabajo
F2	Con los Objetivos de la COAC se encuentra direccionado el centro de cómputo
F12	El personal administrativo tiene el conocimiento adecuado para el uso de los equipos
F8	Bitácoras con todas las incidencias, cambios y procedimientos
F11	El personal dentro del Departamento de Sistemas se encuentra capacitado y es el adecuado ante cualquier problema o requerimiento

Elaborado por: P.A.M.G	**Fecha:** 2019-12-10
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-10

	AUDITORÍA INFORMÁTICA MATRIZ DE PRIORIDADES ARCHIVO CORRIENTE	**MPRI 2/3**

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

MATRIZ DE PRIORIDADES

VARIABLES INTERNAS

Σ	DEBILIDADES
D5	Desactualización de los Equipos Disponibles en la Institución.
D3	No cuenta con gran disposición económica para el mejoramiento de los equipos y los sistemas lo que dificulta la Eficiencia y Eficacia de los trabajadores.
D2	El Personal de Sistemas realiza el mantenimiento solo cuando el equipo o Sistema presenta error o daño
D1	No cuenta con el plan para el desecho de equipos que ya han cumplido con su vida útil
D4	La empresa aun no adquiere ningún seguro, pero en el transcurso del año se lo estará adquiriendo
D6	Las Funciones del personal de Sistemas no se encuentra bien definidas las que no permiten su ejecución de forma eficiente

Elaborado por: P.A.M.G	**Fecha:** 2019-12-10
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-10

	AUDITORÍA INFORMÁTICA MATRIZ DE PRIORIDADES ARCHIVO CORRIENTE	**MPRI 3/3**

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

MATRIZ DE PRIORIDADES

VARIABLES EXTERNAS

∑	**OPORTUNIDADES**
O1	La Adquisición de Nuevas Tecnologías las que permitirán la disminución de Gastos
O2	Uso de Software Libre el que permite mejorar la reducción de Costos y Gastos
O3	Búsqueda de Capacitación por parte de Terceros
O5	En el mercado se encuentra la oferta de Tecnología de punta la que permitirá mejorar la Eficiencia y la Eficacia de la CACECH
O4	Aumento potencial de los salarios de los Socios
∑	**AMENAZAS**
A2	Los precios en el mercado de Software y Hardware son muy elevados
A3	Los Equipos Informáticos se encuentran en evolución constante
A4	Existencia de varios programas corruptos los cuales pueden sabotear y robar información importante de la Institución
A5	Fallos en la energía Eléctrica, o cortes de electricidad sorpresivos
A1	Competencia desleal del mercado

Elaborado por: P.A.M.G	**Fecha:** 2019-12-10
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-10

3.3.2.5. *Perfil Estratégico*

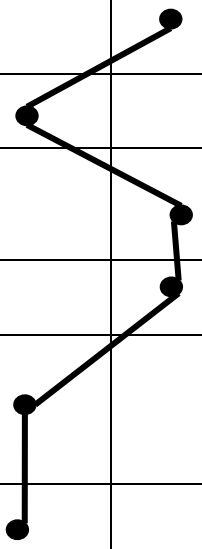
3.3.2.5.1. *Aspectos Internos*

PM Auditor y Consultor	**AUDITORÍA INFORMÁTICA** **PERFIL ESTRATÉGICO** **ARCHIVO CORRIENTE**	**PE 1/3**

ASPECTOS INTERNOS		**CLASIFICACIÓN DE IMPACTO**				
		DEBILIDAD		**NORMAL**	**FORTALEZA**	
		Debilidad	**Gran Debilidad**	**Equilibrio**	**Fortaleza**	**Gran Fortaleza**
		1	**2**	**3**	**4**	**5**
D1	No cuenta con el plan para el desecho de equipos que ya han cumplido con su vida útil					
D2	El Personal de Sistemas realiza el mantenimiento solo cuando el equipo o Sistema presenta error o daño.					
D3	No cuenta con gran disposición económica para el mejoramiento de los equipos y los sistemas lo que dificulta la Eficiencia y Eficacia de los trabajadores.					
D4	La empresa aun no adquiere ningún seguro, pero en el transcurso del año se lo estará adquiriendo					
D5	Desactualización de los Equipos Disponibles en la Institución.					
D6	Las Funciones del personal de Sistemas no se encuentra bien definidas las que no permiten su ejecución de forma eficiente					
F1	El Software utilizado por la empresa se encuentra con licencia y es utilizado.					
F2	Con los Objetivos de la COAC se encuentra direccionado el centro de cómputo.					
F3	La COAC cuenta con conexión a la Red en todo su espacio Físico.					
F4	Posee medidas anti-ataques y filtraciones Informáticas.					
F5	Ambiente laboral idóneo para la realización correcta del trabajo.					
F6	El Sistema informático que cuenta la empresa CONEXUS permite dar seguridad y el funcionamiento adecuado a sus trabajadores, además, otorga a cada empleado lo necesario para cumplir sus actividades.					
Elaborado por: P.A.M.G			**Fecha:** 2019-12-10			
Revisado por: W.G.Y.C H.B.V.S			**Fecha:** 2019-12-10			

	AUDITORÍA INFORMÁTICA PERFIL ESTRATÉGICO ARCHIVO CORRIENTE	PE 2/3

ASPECTOS INTERNOS		CLASIFICACIÓN DE IMPACTO				
		DEBILIDAD		NORMAL	FORTALEZA	
		Debilidad	Gran Debilidad	Equilibrio	Fortaleza	Gran Fortaleza
		1	2	3	4	5
F7	El Software se encuentra direccionado a las necesidades del negocio, actualizado constantemente.					
F8	Bitácoras con todas las incidencias, cambios y procedimientos.					
F9	Documentación necesaria de soporte y los procedimientos informáticos en casi la totalidad de procesos informáticos.					
F10	El Inventario se mantiene actualizado dentro del grupo de activos tecnológicos.					
F11	El personal dentro del Departamento de Sistemas se encuentra capacitado y es el adecuado ante cualquier problema o requerimiento.					
F12	El personal administrativo tiene el conocimiento adecuado para el uso de los equipos					
TOTAL		**2**	**4**	**0**	**5**	**7**
PORCENTAJE		**33.33%**	**66.67%**	**0%**	**41.67%**	**58.33%**



ANÁLISIS DE LOS FACTORES INTERNOS

Del 100% de los factores estratégicos internos el 66.67% corresponde a Gran Debilidad tales como: No cuenta con el plan para el desecho de equipos que ya han cumplido con su vida útil, El Personal de Sistemas realiza el mantenimiento solo cuando el equipo o Sistema presenta error o daño, No cuenta con gran disposición económica para el mejoramiento de los equipos y los sistemas lo que dificulta la Eficiencia y Eficacia de los trabajadores, Desactualización de los Equipos Disponibles en la Institución

El 33.33% corresponde a Debilidades tales como: La empresa aun no adquiere ningún seguro, pero en el transcurso del año se lo estará adquiriendo, Las Funciones del personal de Sistemas no se encuentra bien definidas las que no permiten su ejecución de forma eficiente

Con relación a las Grandes Fortalezas representan el 58.33% en las cuales están: El Software utilizado por la empresa se encuentra con licencia y es utilizado, La COAC cuenta con conexión a la Red en todo su espacio Físico, Posee medidas anti-ataques y filtraciones Informáticas, El Sistema informático que cuenta la empresa CONEXUS permite dar seguridad y el funcionamiento adecuado a sus trabajadores, además, otorga a cada empleado lo necesario para cumplir sus actividades

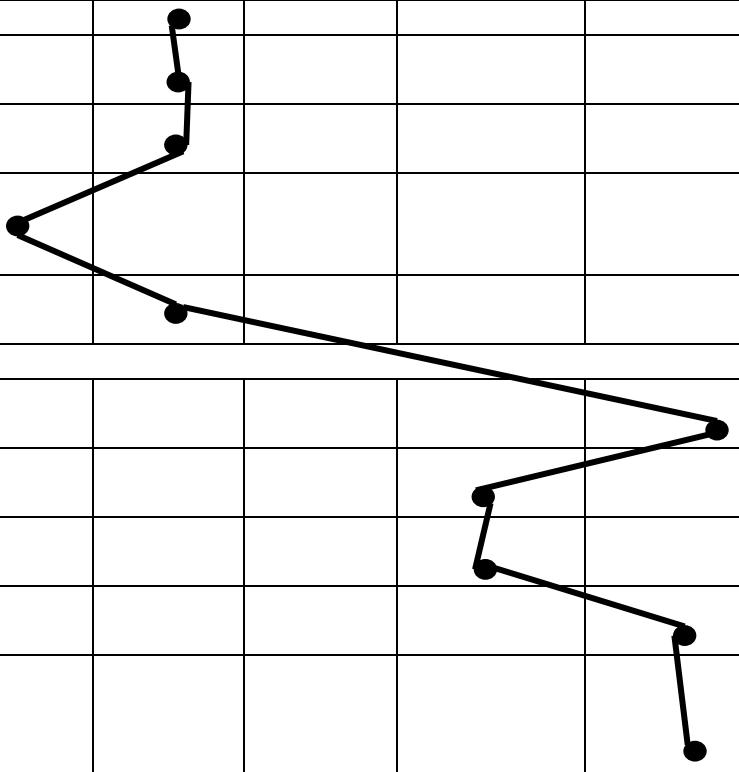
En cambio en las Fortalezas representan el 41.67% en las cuales están: Con los Objetivos de la COAC se encuentra direccionado el centro de cómputo, Ambiente laboral idóneo para la realización correcta del trabajo

Elaborado por: P.A.M.G	**Fecha:** 2019-12-10
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-10

PM Auditor y Consultor	**AUDITORÍA INFORMÁTICA** **PERFIL ESTRATÉGICO** **ARCHIVO CORRIENTE**	**PE 3/3**

3.3.2.5.2. *Aspectos Externos*

ASPECTOS EXTERNOS		**CLASIFICACIÓN DE IMPACTO**				
		AMENAZA		**NORMAL**	**OPORTUNIDAD**	
		Amenaza	**Gran Amenaza**	**Equilibrio**	**Oportunidad**	**Gran Oportunidad**
		1	**2**	**3**	**4**	**5**
A1	Competencia desleal del mercado.					
A2	Los precios en el mercado de Software y Hardware son muy elevados.					
A3	Los Equipos Informáticos se encuentran en evolución constante.					
A4	Existencia de varios programas corruptos los cuales pueden sabotear y robar información importante de la Institución.					
A5	Fallos en la energía Eléctrica, o cortes de electricidad sorpresivos					
O1	La Adquisición de Nuevas Tecnologías las que permitirán la disminución de Gastos.					
O2	Uso de Software Libre el que permite mejorar la reducción de Costos y Gastos.					
O3	Búsqueda de Capacitación por parte de Terceros.					
O4	Aumento potencial de los salarios de los Socios.					
O5	En el mercado se encuentra la oferta de Tecnología de punta la que permitirá mejorar la Eficiencia y la Eficacia de la CACECH					
TOTAL		**1**	**4**	**0**	**2**	**3**
PORCENTAJE		**20%**	**80%**	**0%**	**40%**	**60%**



ANÁLISIS DE LOS FACTORES EXTERNOS

Del 100% de los factores estratégicos externos el 80% corresponde a Gran Amenaza tales como: Competencia desleal del mercado, Los precios en el mercado de Software y Hardware son muy elevados, Los Equipos Informáticos se encuentran en evolución constante, Fallos en la energía Eléctrica, o cortes de electricidad sorpresivos

El 20% corresponde a Amenaza tales como: Existencia de varios programas corruptos los cuales pueden sabotear y robar información importante de la Institución

Con relación a las Grandes Oportunidades representan el 60% en las cuales están: La Adquisición de Nuevas Tecnologías las que permitirán la disminución de Gastos, Aumento potencial de los salarios de los Socios, En el mercado se encuentra la oferta de Tecnología de punta la que permitirá mejorar la Eficiencia y la Eficacia de la CACECH

En cambio en las Oportunidades representan el 40% en las cuales están: Uso de Software Libre el que permite mejorar la reducción de Costos y Gastos, Búsqueda de Capacitación por parte de Tercero

Elaborado por: P.A.M.G	**Fecha:** 2019-12-10
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-10

3.3.2.6. *Matriz de Hallazgos*

	AUDITORÍA INFORMÁTICA MATRIZ DE HALLAZGOS ARCHIVO CORRIENTE	MH 1/5

CONDICION	CRITERIO	CAUSA	EFECTO
Dentro del Manual de Procedimientos no se encuentra de forma escrita el cómo proceder si existe interrupción del Sistema	Dentro de la Norma ISO 27002 dice: 10.10.5: **REGISTRO DE FALLAS** Se debe registrar y analizar las fallas reportadas por los usuarios relacionados con los problemas de procesamiento y comunicación, dando como resultado medidas correctivas y revisar si las acciones fueron tomadas	El personal de la Organización conoce el proceder de cómo Actuar y a quien acudir si existe fallos en el Sistema, pero dentro del manual de Procedimientos no se encuentra detallado el accionar de los Empleados ante tal acontecimiento	Paralización de Actividades y pérdida de Tiempo y de Recursos Económicos
El equipo Informático no se encuentra asegurado.	Dentro de la Norma ISO 27002 dice: 9.1.1: **PERIMETRO DE SEGURIDAD FÍSICA** Se debiera utilizar perímetros de seguridad para proteger las áreas que contienen información y medios de procesamiento de información f) se debiera instalar sistemas de detección de intrusos según estándares nacionales los cuales deben ser probado 9.1.4: **PROTECCION CONTRA AMENAZAS EXTERNAS E INTERNAS** Se debiera considerar el daño por el fuego, inundación, u otras formas de desastres naturales	La Organización contaba hasta fin del año 2017 con el Seguro, ya que culmino el contrato, aunque ya se realizó al primer trimestre del año 2018 el trámite necesario y la documentación para su adquisición, la causa fue por un error humano en la Contratación del Seguro cuya responsabilidad se encontraba por un colaborador que ya no se encuentra laborando en las Instalaciones.	Posibles pérdidas Económicas ante posibles Catástrofes Naturales o por parte de Terceros

Elaborado por: P.A.M.G	**Fecha:** 2019-12-10
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-10

	AUDITORÍA INFORMÁTICA MATRIZ DE HALLAZGOS ARCHIVO CORRIENTE	MH 2/5

CONDICION	CRITERIO	CAUSA	EFECTO
Falta de Comunicación de las Políticas de Seguridad	Dentro de la Norma ISO 27002 dice: 5.1.2: **REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN** La Política de Seguridad deberá ser revisada en intervalos por cualquier cambio significativo. La revisión de la Política de Seguridad deberá tomarse en cuenta los resultados hacia la Gerencia 9.1.5: **TRABAJO EN ÁREAS ASEGURADAS** Se debiera diseñar y aplicar la protección física y los lineamentos necesarios para laborar en áreas aseguradas a) el personal debería estar al tanto de la existencia o las actividades dentro del área asegurada solo conforme a su proceder y lo que necesite conocer. 9.1.6. **ÁREAS DE ACCESO PÚBLICO, ENTREGA Y CARGA** Se debiera controlar los puntos de acceso donde las personas no autorizadas le fuesen negadas el ingreso.	Dentro de la Organización no se estableció buenos canales de información para las Políticas de Seguridad tanto por medios digitales, escritos o comunicados verbales, además ya que no se pudo llegar a un 100% en la comunicación de las Políticas de Seguridad, algunos Empleados de la Organización no cumplen a su totalidad con las mismas, cuyo responsable fue un integrante que ya no se encuentra en funciones	Poner en Riesgo la Seguridad de la Organización, afectar los labores de los Colaboradores de la Organización, posibles fallos del Personal, incumplimiento de las Políticas de Seguridad, perdidas económicas

Elaborado por: P.A.M.G	**Fecha:** 2019-12-10
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-10

	AUDITORÍA INFORMÁTICA MATRIZ DE HALLAZGOS ARCHIVO CORRIENTE	**MH 3/5**

CONDICION	CRITERIO	CAUSA	EFECTO
No cuenta con el plan para la baja de equipos que ya han cumplido con su vida útil	Dentro de la Norma ISO 27002 dice: 9.2.6: **SEGURIDAD DE LA ELIMINACIÓN O RE-USO DEL EQUIPO** Se debiera chequear revisar que los Ítems del equipo que contengan los medios de almacenaje se los retire de los datos confidenciales, destruyéndolos, borrarlos por medio de técnicas las que no permitan por ningún medio volverlas a recuperar 9.2.7: **RETIRO DE PROPIEDAD** El equipo, software no deber retirarse sin la autorización previa correspondiente. b) los usuarios empleados, contratistas y terceras personas que tienen la autoridad para permitir el retiro de los activos fuera del local debieran estar claramente identificados c) se debieran establecer límites de tiempo para el retiro del equipo y se debieran realizar un chequeo de la devolución;	Hasta el final del año analizado la Organización no conto con ningún Plan para la baja o donación de los Equipos que cumplieron su vida Útil dentro de la Empresa, el cual está de responsable en estos momentos el Ing. Carlos Daniel López Martínez quien es el Asistente de Sistemas	Acumulación excesiva en la bodega y perdida de espacio necesario para otras Actividades
El Personal de Sistemas realiza el mantenimiento solo cuando el equipo o Sistema presenta error o daño.	Dentro de la Norma ISO 27002 dice: 9.2.3: **SEGURIDAD DEL CABLEADO** El cableado de la energía y las telecomunicaciones que llevan el Data o dan soporte a los servicios de información debieran protegerse contra los daños 9.2.4: **MANTENIMIENTO DE EQUIPO** Se debiera mantener correctamente el equipo para asegurar su disponibilidad e integridad d) se debieran implementar controles apropiados cuando se programa el equipo para un mantenimiento periódico 15.2.2: **CHEQUEO DEL CUMPLIMIENTO TÉCNICO** Los sistemas de información deberían chequearse regularmente para ver el cumplimiento de los estándares de implementación de la seguridad	La Organización no contaba el año 2018 con un mantenimiento periódico-preventivo el cual pueda evitar el daño o error en los equipos o programas, el responsable es el Ing. Carlos Daniel López Martínez	Perdidas posibles de equipos o Software para la empresa y por ende perdidas económicas
Elaborado por: P.A.M.G		**Fecha:** 2019-12-10	
Revisado por: W.G.Y.C H.B.V.S		**Fecha:** 2019-12-10	

	AUDITORÍA INFORMÁTICA MATRIZ DE HALLAZGOS ARCHIVO CORRIENTE	MH 4/5

CONDICION	CRITERIO	CAUSA	EFECTO
No cuenta con disposición económica para el mejoramiento de los equipos y los sistemas lo que dificulta la Eficiencia y Eficacia de los trabajadores.	Dentro de la Norma ISO 27002 dice: 9.2.4 **MANTENIMIENTO DE EQUIPO** Se debiera mantener correctamente el equipo para asegurar su disponibilidad e integridad a) el equipo se debiera mantener en concordancia con los intervalos y especificaciones de servicio recomendados por el proveedor 10.1.2: **GESTIÓN DE CAMBIO** Se debiera controlar los cambios en los medios y sistemas de procesamiento de la información, además deberían estar sujetos a un estricto control gerencial de cambio a) identificación y registro de cambios significativos b) planeación y prueba de cambios c) evaluación de los impactos potenciales de los cambios, incluyendo los impactos de seguridad	La Organización no dispuso la cantidad adecuada para la renovación y actualización de equipos y programas informáticos, el responsabilidad cae sobre un colaborador que ya no se encuentra en la empresa	Desactualización a Nivel Informático y especialización en Tics del Personal
Desactualización de los Equipos disponibles en la Institución	Dentro de la Norma ISO 27002 dice: 7.1.3: **USO ACEPTABLE DE LOS ACTIVOS** Se debe identificar, documentar e implantar reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la información	Por la falta de parte económica los equipos en el año 2018 no se encontraban en las mejores condiciones para la realización de labores de carácter normal de la empresa, la responsabilidad se encuentra en manos de la Ing. Gabriela Elizabeth Rodríguez Santos	Posibilidad de Interferencias en los Labores de los Colaboradores, y desactualización Tecnológica para los Servicios que brinda la Empresa

Elaborado por: P.A.M.G	**Fecha:** 2019-12-10
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-10

	AUDITORÍA INFORMÁTICA MATRIZ DE HALLAZGOS ARCHIVO CORRIENTE	MH 5/5

CONDICIÓN	CRITERIO	CAUSA	EFECTO
Las Funciones del personal de Sistemas no se encuentran definidas las que no permiten su ejecución de forma eficiente.	Dentro de la Norma ISO 27002 dice: 6.1.3. **ASIGNACIÓN DE LA RESPONSABILIDAD DE LA INFORMACIÓN** Todas las responsabilidades de la seguridad de la información deberían estar claramente definidas, se debería definir claramente las responsabilidades para la protección de los activos individuales y llevar a cabo los procesos de seguridad especifico 8.1.1. **ROLES Y RESPONSABILIDADES** Se debiera 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.	Dentro del manual de Funciones que posee la empresa no se encuentra bien definida los Deberes de los Empleados del Departamento, la responsabilidad recae en la Ing. Gabriela Elizabeth Rodríguez Santos	Duplicidad de Funciones, Perdidas de Tiempos en Otras Actividades, Perdidas Económicas a la Organización

Elaborado por: P.A.M.G	**Fecha:** 2019-12-10
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2019-12-10

FASE III: Informe de Auditoría

3.3.3. *Informe de Auditoría*

3.3.3.1. *Carta de Presentación*

	AUDITORÍA INFORMÁTICA **CARTA DE PRESENTACIÓN** **INFORME FINAL** **ARCHIVO CORRIENTE**	**CPIF 1/1**

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

Riobamba, 30 de enero de 2020

Ingeniero

Ramiro Fabián Tobar Esparza

GERENTE GENERAL

Presente.-

De mi consideración:

Una vez realizada la Auditoria Informática a la Cooperativa que usted brinda un soporte esencial y encamina a la excelencia de manera muy eficiente.

Comunico que se realizó el análisis en base al marco de referencia del COSO 2 y las Normas ISO 27002, el que se enfocó principalmente para el gobierno de las TI y lograr verificar si existen desviaciones en los Controles Aplicados durante dicho análisis.

Por consiguiente le presento a Usted el Informe Final de la Auditoria con las respectivas recomendaciones.
Atentamente

Paúl Alejandro Merizalde Guamanzara
Gerente de PM Auditor y Consultor

Elaborado por: P.A.M.G	**Fecha:** 2020-01-09
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2020-01-09

3.3.3.2. *Informe Final*

	AUDITORÍA INFORMÁTICA **INFORME FINAL** **ARCHIVO CORRIENTE**	**IF 1/6**

Organización:	CACECH
Naturaleza del trabajo:	Auditoría Informática
Período:	Año 2018

INFORME DE AUDITORÍA INFORMÁTICA CACECH

Motivo del examen

El examen se lo desarrollo para verificar la situación actual de la Organización específicamente en el uso y aprovechamiento de las TIC en la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo Ltda.", en la misma valoró los ocho Procesos que considera las normas del COSO 2 y son: Ambiente Interno, Establecimiento de Objetivos, Identificación de Eventos, Evaluación de Riesgo, Respuesta al Riesgo, Actividades de Control, Información y Comunicación y Monitoreo. Cada uno de los aspectos se la Aplico a toda la Organización.

Objetivo General

Aplicar una Auditoría Informática a la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda., de la Ciudad de Riobamba., periodo 2018, mediante la información emitida por la Institución facilitadora, y con eso expresar un informe de Auditoria el cual servirá de herramienta para la toma de decisiones Gerenciales.

Elaborado por: P.A.M.G	**Fecha:** 2020-01-09
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2020-01-09

	AUDITORÍA INFORMÁTICA **INFORME FINAL** **ARCHIVO CORRIENTE**	**IF 2/6**

Organización:	CACECH
Naturaleza del trabajo:	Auditoría Informática
Período:	Año 2018

Objetivos específicos

Elaborar el marco teórico con la utilización de fuentes bibliográficas actualizada y especializada, de tal forma que sirvan para sustentar la presente investigación.

Efectuar la recopilación de la Información necesaria y la aplicación del COSO II (E.R.M), a través de las fuentes de primarias y secundarias, y con esto recabar los datos necesarios para la Investigación.

Ejecutar la Auditoría Informática al Área de Sistemas de la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda., de la Ciudad de Riobamba, periodo 2018, mediante la información emitida por la Institución facilitadora, y con eso presentar un informe de Auditoria el cual servirá de herramienta para la toma de decisiones Gerenciales.

Alcance

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

Base Legal

Se aplicó:

Componentes del COSO II

Normas ISO 27002

Elaborado por: P.A.M.G	**Fecha:** 2020-01-09
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2020-01-09

	AUDITORÍA INFORMÁTICA **INFORME FINAL** **ARCHIVO CORRIENTE**	**IF 3/6**

Organización:	CACECH
Naturaleza del trabajo:	Auditoría Informática
Período:	Año 2018

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

MISION

Brindar servicios financieros de excelencia y calidad a los Servidores Públicos del Sistema Educativo de la Provincia de Chimborazo, a sus cónyuges e hijos, mediante un servicio ágil y personalizado, manteniendo la solidez y eficiencia que siempre nos ha caracterizado

VISION

Seguir siendo la mejor y más sólida Cooperativa del Sistema Educativo, mediante la prestación de servicios financieros de calidad, excelencia y una administración eficiente. Mantener un equipo de trabajo efectivo entre Directivos, Representantes, Colaboradores y asociados, que contribuya con el desarrollo financiero, económico, tecnológico y empresarial de la CACECH

VALORES INSTITUCIONALES Y CULTURA INTERNA

Vocación de Servicio para satisfacer al Cliente: Es una actitud del personal de la CACECH, para atender las necesidades de los socios y clientes para satisfacer sus expectativas.

Actitud de Liderazgo: Buscamos el mejoramiento continuo, para constituirnos en el mejor referente del desarrollo de la economía social y solidaria del magisterio ecuatoriano.

Elaborado por: P.A.M.G	**Fecha:** 2020-01-09
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2020-01-09

Honestidad.- Trabajamos con honradez, dignidad, equidad, solidaridad y modestia.

Trabajo en Equipo: Complementamos y potenciamos las iniciativas, los conocimientos y recursos individuales, para hacerlo mejor. Trabajando en equipo, cada día lo hacemos más y mejor.

Competitividad: Ofrecemos productos y servicios competitivos de calidad, con eficiencia y eficacia, tenemos servicios y productos de calidad, al alcance de todos los socios.

Generadores de desarrollo sustentable: Con nuestros servicios propiciamos el desarrollo y mejoramos la calidad de vida de los servidores públicos del sistema educativo de la provincia, sus cónyuges e hijos, la colectividad, hoy y siempre. Contribuimos al bienestar y progreso de la familia CACECH

	AUDITORÍA INFORMÁTICA INFORME FINAL ARCHIVO CORRIENTE	IF 5/6

Organización: CACECH
Naturaleza del trabajo: Auditoría Informática
Período: Año 2018

HALLAZGOS DE AUDITORÍA Y RECOMENDACIONES

1. Dentro del Manual de Procedimientos no se encuentra de forma escrita el cómo proceder si existe interrupción del Sistema

El personal de la Organización conoce el proceder de cómo actuar y a quien acudir si existe fallos en el Sistema, pero dentro del manual de procedimientos no se encuentra detallado el accionar de los empleados ante tal acontecimiento.

Recomendación

- A la Gerencia: Revisión de los Manuales de Procedimientos disponibles en la Organización, monitoreo de los procedimientos realizados por los Colaboradores en los puestos de Trabajo asignados.

- A la Administración en Sistemas: Solicitar que todos los Procedimientos que se vayan a ejercer se encuentren estipulados dentro de los manuales Correspondientes.

2. El equipo Informático no se encuentra asegurado.

La Organización contaba hasta fin del año 2017 con el Seguro, ya que culmino el contrato, aunque ya se realizó al primer trimestre del año 2018 el trámite necesario y la documentación para su adquisición.

Recomendación

- A la Gerencia: Tener una comunicación y revisión constante del periodo de Vigencia de los Contratos para evitar gastos innecesarios, asignar a un Colaborador la revisión.

Elaborado por: P.A.M.G	**Fecha:** 2020-01-09
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2020-01-09

	AUDITORÍA INFORMÁTICA **INFORME FINAL** **ARCHIVO CORRIENTE**	**IF 6/6**

Organización:	CACECH
Naturaleza del trabajo:	Auditoría Informática
Período:	Año 2018

3. Falta de Comunicación de las Políticas de Seguridad

Dentro de la Organización no se estableció buenos canales de información para las Políticas de Seguridad tanto por medios digitales, escritos o comunicados verbalmente, además ya que no se pudo llegar a un 100% en la comunicación de las Políticas de Seguridad, algunos Empleados de la Organización no cumplen a su totalidad con las mismas

Recomendación

- A la Gerencia: Dar las Funciones a un Colaborador de revisión y cumplimiento de las Políticas de Seguridad y colocar respectivas sanciones por incumplimiento, establecer buenos canales de Comunicación Interno para la Organización logrando alcanzar a todos los colaboradores, organizar un conversatorio con el fin de dispersión de las Políticas

- A la Administración en Sistemas: Controlar las Políticas de Seguridad Área por Área y brindar el debido asesoramiento de las mismas

Elaborado por: P.A.M.G	**Fecha:** 2020-01-09
Revisado por: W.G.Y.C H.B.V.S	**Fecha:** 2020-01-09

4. No cuenta con el plan para la baja de equipos que ya han cumplido con su vida útil

Hasta el final del año analizado la Organización no conto con ningún Plan para la baja o donación para los equipos que cumplieron su vida útil dentro de la Empresa

Recomendación

- A la Gerencia: Promover la Reutilización del Equipo que se encuentre operativo pero ya no sea de utilidad para la empresa a través de la planificación y elaboración de un Plan de Baja o se Proceda a una Donación de Equipo no en Funciones

- A la Administración en Sistemas: Conciliar los Equipos que se encuentren dados de baja y presentar un Informe a la Gerencia para la decisión Final

5. El Personal de Sistemas realiza el mantenimiento solo cuando el equipo o Sistema presenta error o daño

La Organización no contaba el año 2018 con un mantenimiento periódico-preventivo el cual pueda evitar el daño o error en los equipos o programas

Recomendación

- A la Gerencia: Controlar y proponer lineamientos de Mantenimiento periódico a los equipos evitándose así costos y gastos innecesarios

6. No cuenta con disposición económica para el mejoramiento de los equipos y los sistemas lo que dificulta la Eficiencia y Eficacia de los trabajadores

La Organización no dispuso la cantidad adecuada para la renovación y actualización de equipos y programas informáticos

Recomendación

A la Gerencia: Analizar y Redistribuir el Presupuesto Disponible en la Organización para su ejecución en posibles nuevas adquisiciones.

A la Administración en Sistemas: Revisar la actual Necesidad de equipo informático

y presentar un plan para adquirirlos a través de la revisión de varias proformas

7. Desactualización de los Equipos disponibles en la Institución

Por la falta de parte económica los equipos en el año 2018 no se encontraban en las mejores condiciones para la realización de labores de carácter normal de la empresa

Recomendación

A la Gerencia: Destinar el recurso Económico de mejor manera priorizando en Equipos Informáticos

8. Las Funciones del personal de Sistemas no se encuentran definidas las que no permiten su ejecución de forma eficiente

Dentro del manual de Funciones que posee la empresa no se encuentra bien definida los Deberes de los Empleados del Departamento

Recomendación

Ala Gerencia: Replantear el manual de Funciones del personal de Sistemas, especificando cada puesto y obligación.

CONCLUSIONES

- Después de la planificación, ejecución y la realización del debido informe de Auditoría Informática a la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda. aplicando como marco de referencia el COSO II y para el análisis la norma ISO 27002, permitieron entregar dicho informe con las debidas conclusiones y recomendaciones para mejorar la eficiencia, la eficacia y la economía dentro de la Organización.

- Se realizó la estructuración del marco teórico referencial para que este trabajo de investigación se encuentre en base de a lineamientos lo que permite decir que no es improvisado, permitiendo distribuir mejor los recursos disponibles en la empresa asegurando que los resultados sean confiables, lógicos y comparables

- Las fallas fueron identificadas a través de la aplicación del COSO II y la norma ISO 27002, y se recomendaron acciones que permitirán corregir los errores a corto plazo de una manera efectiva en relación al software, hardware, infraestructura, seguridad y mantenimiento informático de la COAC.

- Dentro de la investigación existen varios hallazgos, siendo el más relevante, la falta de socialización de las políticas de seguridad, porque el responsable no las comunicó a tiempo, provocando su salida de la empresa.

RECOMENDACIONES

- A la Administración de la empresa, contratar auditorías que le permita completar la revisión de los sistemas informáticos de la Cooperativa de Ahorro y Crédito "Educadores de Chimborazo" Ltda., con el fin de propender al cumplimiento de los objetivos organizacionales.

- Implementar un plan de acción para materializar el cumplimiento de las recomendaciones citadas en el informe de auditoría, minimizando el riesgo existente.

- Revisar el manual de funciones del personal para optimizar las actividades de los colaboradores de la organización logrando eficiencia y evitando duplicidad de esfuerzos.

- Socializar el manual de seguridad a todos los colaboradores de la organización, evitando posibles daños en los activos de la empresa y fomentar la salud ocupacional.

GLOSARIO

Software: Son instrucciones (programas de computadora) que cuando ejecutado proporcionan características, función y rendimiento deseados; estructuras de datos que permiten a los programas manipular adecuadamente información. (Pressman, R., 2015, p. 4)

Hardware: En computación e informática, se conoce como hardware (unión de los vocablos del inglés hard, rígido, y ware, producto, mercancía) al total de los elementos materiales, tangibles, que forman al sistema informático de una computadora u ordenador dentro de la organización. (Raffino, E., 2020, p. 35)

Auditoría: es la acumulación y evaluación de evidencia basada en información para determinar y reportar sobre el grado de correspondencia entre la información y los criterios establecidos. La auditoría debe realizarla una persona independiente y competente. (Arens, A., 2007, p. 4)

Informática: Ciencia del tratamiento sistemático y eficaz, realizado especialmente mediante máquinas automáticas, de la información contempladas como vehículo de saber humano, y de la comunicación de los ámbitos técnico, económico y social. (Echenique J., 2009, p. 3)

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. (Muñoz, C., 2002, p. 19)

COSO II (E.R.M.): Proceso, efectuado por la junta de directores de una entidad, por la administración y por otro personal, aplicado en el establecimiento de la estrategia y a través del emprendimiento, diseñado para identificar los eventos potenciales que puedan afectar la entidad, y para administrar los riesgos que se encuentran dentro de su apetito por el riesgo, a fin de proveer seguridad razonable en relación con el logro del objetivo de la entidad. (Estupiñan, R., 2015, p. 119).

Enfoque de investigación cualitativa: Profundiza 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. (Bonilla, E., 2005, p.60)

BIBLIOGRAFIA

Arens, A. A. (2007). *Auditoría: un enfoque integral.* Juárez, México: Pearson

Azofra, M. (1999). *Cuestionarios.* Recuperado de https://metodologiadelainvestigacionii.files.wordpress.com/2012/08/unidad4-azofra-cuestionarios.pdf

Behar, D. (2008). *Metodología de la Investigación.* México: Shalom

Bonilla, E. (2005). *Más allá del dilema de los métodos.* Bogotá, Colombia: Nomos

Calduch, R. (2014). *Métodos y técnicas de investigación en relaciones internacionales* (tesis de doctorado). Universidad Complutense de Madrid. España

Cañedo, R. (2005). *La Informática, la Computación y la Ciencia de la Información: una alianza para el desarrollo.* Acimed, 13(5). Recuperado de http://bvs.sld.cu/revistas/aci/vol13_5_05/aci07505.htm

Caurin, J. (2018). La organización de la empresa. *Emprende pyme.net.* Recuperado de https://www.emprendepyme.net/la-organizacion-de-la-empresa

Chiavenato, I. (2000). *Administración de recursos humanos.* Bogotá, Colombia: McGraw-Hill

Echenique, J. A. (2009). *Auditoría en informática.* México: McGraw-Hill

Espinosa, R. (2019). *La matriz de análisis DAFO (FODA).* Recuperado de https://robertoespinosa.es/2013/07/29/la-matriz-de-analisis-dafo-foda

Estupiñan, R. (2015). *Administración de riesgos E. R. M. y la auditoría interna.* Bogotá, Colombia: Ecoe Ediciones

Fidias, G. (2012). *El proyecto de investigación introducción a la metodología científica.* Caracas, Venezuela: Episteme C. A.

Ghafran, C. (2017). *The Governance Role of Audit Committees.* 15: 381-407. doi:10.1111/j.1468-2370.2012.00347.x

Graterol, R. (2011). *Metodología de la investigación.* Venezuela: Ateproca

Hernández, R. (2010). *Metodología de la investigación.* México: McGraw-Hill

Internacional Laboratory Acreditacion Cooperation (ILAC). (2016) ¿Qué es la inspección?..*ILAC.* Recuperado de http://ilac.org/?ddownload=2248

ISO (2013). *ISO/IEC 27001:2013.* Information technology Security techniques Information security management systems. Requirements. Ginebra: International Standardisation Organisation.

Méndez, C. (2003). Metodología para describir la cultura corporativa. *Cuadernos de Administración, 16*(25), 139-171. ISSN: 0120-3592. Recuperado de: https://www.redalyc.org/articulo.oa?id=205/20502507

Monje, C. (2011). *Metodología de la investigación cuantitativa y cualitativa guía didáctica.* Colombia: Neiva

Muñoz, C. (2002). *Auditoría en sistemas computacionales.* Mexico: Pearson

NIA 200

Osorio, R. (1990). El cuestionario. *Centro de estudio de opinión.* Recuperado de https://revistas.udea.edu.co/index.php/ceo/article/download/1498/1155/

Pérez, G. (2009). *Metodología de la investigación educativa, un acercamiento desde la perspectiva del maestro.* Lima: San Marcos.

Pinilla, J. (1994*). Las normas de auditoría informática*. INNOVAR, 4, 31-34. DOI: http://dx.doi.org/10.15446/innovar

Plummer, K. (1989). *Los documentos personales. Introducción a los problemas y la bibliografía del método humanista.* España: Siglo XXI Editores.

Porter, L. W. (1983). *Motivation and Work Behavior.* New York: McGraw-Hill

Pressman, R. (2015) *Software Engineering: A practitioner's approach*. New York, USA: McGraw-Hill.

Raffino, E. (2020, 1 de junio). Concepto de Hardware. *Concepto.de.* Recuperado de https://concepto.de/hardware/

Raffino, M. (2020). Investigar. *Concepto.de.* Recuperado de https://concepto.de/investigar

Rodríguez, M. (19 de agosto de 2013). Acerca de la investigación bibliográfica y documental. *Guía de Tesis.* Recuperado de https://guiadetesis.wordpress.com/2013/08/19/acerca-de-la-investigacion-bibliografica-y-documental/#comments

Whittington, P. (2005). *Principios de auditoria.* México: McGraw-Hill

ANEXOS

ANEXO A: Inventario Físico y Lógico

Área	Usuario	Cargo	N.	Activo Fijo	Descripción	Marca	Serie	Estado Físico
Contabilidad	Remache Yaulema Karina Alexandra	Contadora	1	Monitor	Pantalla plana 18,0” LCD	COMPAQ	CNC017PKFJ	Bueno
			2	CPU	2 GB RAM / 465 GB HDD Procesador Intel i3 / 32 bits	HP	MXL0382C45	Regular
			3	Teclado	Latam. / Alfanumérico / USB	HP		Bueno
			4	Mouse	Láser / 3 botones / scroll / USB	HP		Bueno
			5	Impresora	LaserJet P2055dn / Monocrom.	HP	CN9053647	Bueno
	Hernández Vaca Verónica Lorena	Asistente 1	6	Monitor	Pantalla plana 18,0” LCD	HP	CNC013Q7BD	Bueno
			7	CPU	2 GB RAM / 253 GB HDD Procesador Intel i3 / 32 bits	HP	MXL039052R	Bueno
			8	Teclado	Latam. / Alfanumérico / USB	HP		Bueno
			9	Mouse	Láser / 3 botones / scroll / USB	HP		Bueno
	Rosero Viñan Myriam del Carmen	Asistente 2	10	Monitor	Pantalla plana 17,0” Color	SAMSUNG	PE16H9NQ811125J	Bueno
			11	CPU	2 GB RAM / 216 GB HDD Procesador Intel Core 2 Duo / 32 bits	HP	MXJ91500XP	Bueno
			12	Teclado	Latam. / Alfanumérico / PS2	HP		Bueno
			13	Mouse	Láser / 3 botones / scroll / PS2	HP		Bueno
	Uso exclusivo		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 exclusivo		15	Computador Portátil	4 GB RAM / 465 GB HDD Procesador Intel i5 / 64 bits	HP	CNU0432PGX	Bueno
	Uso practicantes		16	Monitor	Pantalla plana 18,0” LCD	HP	6CM420283N	Bueno
			17	CPU	4 GB RAM / 464 GB HDD Procesador Intel i5 / 64 bits	HP	MXL41212G5	Bueno
			18	Mouse	Láser / 3 botones / scroll / USB	HP	FCMHH0CJP6B4LU	Bueno
			19	Teclado	Latam. / Alfanumérico / USB	HP		Bueno
	Uso general		20	Copiadora	4 bandejas / WorDcentre 5845	XEROX	152506400	Bueno
Créditos	Tipan Holguin Veronica Paola--		21	Monitor	Pantalla plana 18,0” LCD	HP	6CM42028F8	Bueno
			22	CPU	4 GB RAM / 465 GB HDD Procesador Intel i5 / 64 bits	HP	MLX41212G1	Bueno
			23	Mouse	Láser / 3 botones / scroll / USB	HP	67436-001	Bueno
			24	Teclado	Latam. / Alfanumérico / USB	HP	724720-161	Bueno
			25	Impresora	LaserJet M401dw / Monocrom.	HP	VNB3D09226	Bueno
			26	Impresora	Matriz de punto / Monocrom.	EPSON	CDUY239173	Bueno
Presidencia	Saltos Urquizo Elvia Marina	Secretaria	27	Monitor	Pantalla cuadrada 17,0”	HP	3CQ9070Y3G	Bueno
			28	CPU	2 GB RAM / 232 GB HDD Procesador Intel Core 2 Duo / 32 bits	HP	MXJ91407ZY	Bueno
			29	Mouse	Láser / 3 botones / scroll / PS2	HP	FB7330AN3X020XE	Bueno
			30	Teclado	Latam. / Alfanumérico / PS2	HP	BC3370GVBWY7VR	Bueno

Área	Usuario	Cargo	N.	Activo Fijo	Descripción	Marca	Serie	Estado Físico
Consejo de administrac.	Saltos Urquizo Elvia Marina	Secretaria	31	Monitor	Pantalla plana 18,0” LCD	HP	6CM3462FC0	Bueno
			32	CPU	4 GB RAM / 464 GB HDD Procesador Intel i7 / 64 bits	HP	MXL4081JCL	Bueno
			33	Mouse	Láser / 3 botones / scroll / USB	HP	FCMHF0A9W55979	Bueno
			34	Teclado	Latam. / Alfanumérico / USB	HP	BDMEP0CVB5SS4N	Bueno
			35	Impresora	LaserJet M1319 / Monocrom.	HP	CNJ99C0B05	Bueno
Captaciones	Yungan Yaucan Jenny Patricia	Oficial de captaciones	36	Monitor	Pantalla plana 18,0” LCD	HP	6CM3462CNC	Bueno
			37	CPU	4 GB RAM / 464 GB HDD Procesador Intel i7 / 64 bits	HP	MXL4081K4B	Bueno
			38	Mouse	Láser / 3 botones / scroll / USB	HP	FCHHF0A9W559SL	Bueno
			39	Teclado	Latam. / Alfanumérico / USB	HP		
			40	Impresora	LaserJet M1319 / Monocrom.	HP	CNB1M14687	Bueno
	Romero Berrones Andrea Paulina	Asistente de Crédito 1	41	Monitor	Pantalla plana 18,0” LCD	HP	6CM3462CNB	Bueno
			42	CPU	4 GB RAM / 464 GB HDD Procesador Intel i7 / 64 bits	HP	MXL4081JCK	Bueno
			43	Mouse	Láser / 3 botones / scroll / USB	HP	FCMHF0A9W5597K	Bueno
			44	Teclado	Latam. / Alfanumérico / USB	HP	BDMEP0CVB5X3Z9	Bueno
			45	Impresora	LaserJet 1018 / Monocrom.	HP		Bueno

Área	Usuario	Cargo	N.	Activo Fijo	Descripción	Marca	Serie	Estado Físico
Créditos	Telenchano Ilbay Franklin Ernesto	Asistente de Crédito 2	46	Monitor	Pantalla plana 18,0” LCD	HP	6CM3462CVJ	Bueno
			47	CPU	4 GB RAM / 465 GB HDD Procesador Intel i5 / 64 bits	HP	MXL4081JC6	Bueno
			48	Mouse	Láser / 3 botones / scroll / USB	HP	FCMHF0A9W55994	Bueno
			49	Teclado	Latam. / Alfanumérico / USB	HP	BDMEP0CVB5S01I	Bueno
			50	Impresora	LaserJet M401dw / Monocrom.	HP	CNB9M09613	Bueno
			51	Impresora	Matriz de punto / Monocrom.	EPSON	G8DY494081	Bueno
Auditoría	Barrionuevo Tacuri Jacqueline Alexandra	Auditoría Interna	52	Monitor	Pantalla plana 18,0” LCD	COMPAQ	CNC013Q7C2	Bueno
			53	CPU	2 GB RAM / 297 GB HDD Procesador Intel i3 / 32 bits	HP	MXL0382C5X	Bueno
			54	Mouse	Láser / 3 botones / scroll / USB	HP		Bueno
			55	Teclado	Latam. / Alfanumérico / USB	HP	BBAWE0JGAYY01W	Bueno
			56	Impresora	LaserJet P2015dn / Monocrom.	HP	CNBJM67155	Bueno
Caja	Hernández Buenaño Marcia Lorena	Jefe caja	57	Monitor	Pantalla plana 18,0” LCD	COMPAQ	CNT939CKMC	Bueno
			58	CPU	2 GB RAM / 298 GB HDD Procesador Intel Core2 Quad / 64 bits	HP	MXJ94603V4	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	Zabala Parreño Fernanda Verónica	Cajera	65	Monitor	Pantalla plana 18,0” LCD	COMPAQ	CNT939CKLT	Bueno
			66	CPU	2 GB RAM / 298 GB HDD Procesador Intel Core2 Quad / 32 bits	HP	MXJ94603TY	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	Aguirre Niama Carla Gabriela	Cajera, Asistente TI	70	Monitor	Pantalla plana 18,0” LCD	HP	6CM21314YP	Bueno
			71	CPU	2 GB RAM / 281 GB HDD Procesador Intel Core2 Quad / 32 bits	HP	MXJ94603V3	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

Área	Usuario	Cargo	N.	Activo Fijo	Descripción	Marca	Serie	Estado Físico
Secretaría general	Ortiz Coronel Vilma Susana	Secretaria General	78	Monitor	Pantalla plana 18,0” LCD	HP	6CM3462F42	Bueno
			79	CPU	4 GB RAM / 465 GB HDD Procesador Intel i7 / 64 bits	HP	MXL4081K4H	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	Rodriguez Santos Gabriela Elizabeth	Admin. de Sistemas	84	Monitor	Pantalla plana 18,5” LCD	COMPAQ	CNC013Q7B0	Bueno
			85	Monitor	Pantalla plana 18,5” LCD	HP	6CM3462D20	Bueno
			86	Monitor de vigilancia	Pantalla plana 40,0” LED	HP	CNV5764F01	Bueno
			87	CPU	16 GB RAM / 464 GB HDD Procesador Intel i7 / 64 bits	HP	MXL4081JVC	Bueno
			88	CPU	8 GB RAM / 297 GB HDD Procesador Intel i3 / 64 bits	HP	MXL039052L	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, 8 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
Sistemas	López Martínez Carlos Daniel	Asistente de Sistemas	98	Monitor	Pantalla plana 18,5” LCD	HP	8CM3462D10	Bueno
			99	CPU	8 GB RAM / 464 GB HDD Procesador Intel i7 / 64 bits	HP	MXL4811JVC	Bueno
			100	Mouse	Láser / 3 botones / scroll / USB	HP	FCMHF0A9S4197X	Bueno
Gerencia	Tobar Esparza Ramiro Fabián	Gerente general	101	Computador Portátil	8GB RAM / 750GB RAM Intel i7 / 64 bits	HP	2CE20927FQ	Bueno
			102	Computador Portátil	8GB RAM / 1 TB RAM Intel i3 / 64 bits	HP	CND5114805	Bueno
			103	Adaptador computador portátil	Salida 6.5 a 120 W para portátil DV6	HP	WBGTE0BHH105RK	Bueno
			104	Impresora	LaserJet 1320, Monocrom. 2 bandejas	HP	CNHC5D10YM	Bueno
			105	Impresora	LaserJet CP2025, Color 2 bandejas	HP	CNGS204881	Bueno
			106	Regulador de voltaje	8 tomas, FVR 1211B	FORZA	09310931314	Bueno
			107	Disco duro externo	500 GB/7200 RPM/ APOLLO M100	IMATION		Bueno
			108	Proyector	2700 Lumens/ 1280*800 HDMI/ Lápiz óptico	INFOCUS	BFJM112A1391	Bueno
			109	Proyector	S18+	EPSON	V9TK5210354	Bueno

Área	Usuario	Cargo	N.	Activo Fijo	Descripción	Marca	Serie	Estado Físico
			110	Ventilador para computador portátil	5 posiciones / 4 entradas USB 2.0 / silencioso	ERGOS TAND		Bueno
			111	Hub	4 entradas USB / azul	R-LIP		Bueno
Se totalizan 111 artículos en la toma física realizada.								

Fuente: Toma física

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

ANEXO B: Software de la Empresa

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		6.1.0	**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 10 Pro		SP2	6	X		X	
2	Windows 8 Professional		SP1	6	X		X	
3	Windows 8 Home Premium		SP1	5	X		X	
4	Windows 7		SP3	4	X		X	
5	Centos 6 Server			2	X		X	
6	Windows 2015 Server Edition			1	X		X	
7	Windows 2015 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 Lógica

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

Encuestas aplicadas

ANEXO C: Encuestas Aplicadas

a) SEGURIDAD LÓGICA (Jefa de Sistemas)

CUESTIONARIO	SI	NO	N/A	OBSERVACION	MARCAS
Ambiente Interno					
21. ¿Se adquiere las licencias necesarias para el uso de todos los Programas disponibles en la Organización?	✓			**Si**	✓
22. ¿La empresa posee un antivirus para evitar posibles fallos en el sistema?	✓			**Si**	✓
23. ¿La Organización posee un Cortafuegos debidamente Configurado el cual evite accesos de terceros?	✓			**Si**	✓
24. ¿La Contraseña posee un número mínimo de caracteres?	✓			**Si**	✓
25. ¿Cuándo finaliza los Labores de un empleado, se da de baja su acceso?	✓			**Si**	✓
Establecimiento de Objetivos					
26. ¿Los programas se encuentran actualizados?	✓			**Si (Cada vez que existe un parche de actualización)**	✓
27. ¿Los programas para detección se mantienen actualizados?	✓			**Si (De forma automática)**	✓
Identificación de Eventos					
28. ¿Existen un registro o logs que permitan conocer si existen accesos no autorizados?	✓			**Si**	✓
29. ¿Los Usuarios solo tienen disponible los módulos para su labor?	✓			**Si (Solo se activan los módulos necesarios para el desempeño de los labores)**	✓
Evaluación de Riesgos					
30. ¿Revisa de manera regular los programas instalados?		✓		**No (Cuando existe algún fallo realizan la revisión)**	*
31. ¿El nivel de Seguridad en las Contraseñas constan: números, letras, signos de puntuación, caracteres especiales?	✓			**Si (A excepción los signos de puntuación)**	✓

CUESTIONARIO	SI	NO	N/A	OBSERVACION	MARCAS
Respuesta al Riesgo					
32. ¿Se tiene previsto en el plan de contingencias, como actuar si existe modificaciones de claves no previstas?		✓		**No (Dentro del Plan de Contingencias no existe esta previsión)**	*
33. ¿Se modifica de manera constante las Claves de acceso?	✓			**Si (El Sistema lo solicita cada 30 Días)**	✓
Actividades de Control					
34. ¿Poseen los equipos medios de seguridad tales como: claves de acceso?	✓			**Si**	✓
35. ¿Realiza un seguimiento de las Operaciones?	✓			**Si (Tres veces a la Semana)**	✓
36. ¿Existe limitantes de acceso en los Intentos Fallidos?	✓			**Si (3 veces lo permite el Sistema)**	✓
Información y Comunicación					
37. ¿Se tiene un Control para la revisión de los mecanismos de seguridad?	✓			**Si (El control se lo realiza una vez a la semana)**	✓
38. ¿Cada Usuario se Identifica su acceso?	✓			**Si**	✓
Monitoreo					
39. ¿En alguna ocasión en el periodo auditado se ha encontrado algún programa malicioso?		✓		**No**	✓
40. ¿En los Ficheros se almacena Datos de Carácter Personal de los Usuarios?		✓		**Los ficheros no permiten el almacenamiento de estos Datos**	✓

b) SEGURIDAD FÍSICA (Jefa de Sistemas)

CUESTIONARIO	SI	NO	N/A	OBSERVACION	MARCAS
Ambiente Interno					
32. ¿La organización cuenta con copias o respaldos físicos?	✓			**Se encuentran en la bóveda de la Organización y en una Caja de Seguridad en el Banco del Austro.**	✓ 🕮
33. ¿El centro de cómputo se encuentra conectada al exterior?	✓				✓
34. ¿La Seguridad es Contratada?	✓			**Para la seguridad se establece un Contrato de servicios profesionales**	✓ 🕮
35. ¿La Organización cuenta con salida de Emergencia?	✓				✓
36. ¿El cableado de la Red se encuentra debidamente instalado?	✓				✓
Establecimiento de Objetivos					
37. ¿En el Departamento de Sistemas existe prohibición de consumo de alimentos y bebidas para evitar los posibles daños y averías?	✓				✓ 🕮
38. ¿No existen obstáculos, se encuentran al alcance y están debidamente etiquetados los interruptores de Luz?	✓				✓
39. ¿Posee una clasificación de la Información, y como se la clasifica dentro de la Organización?	✓			**c) Vital: Base de datos, instaladores, claves, reportes** **d) Esencial: Información**	✓ 🕮

CUESTIONARIO	SI	NO	N/A	OBSERVACION	MARCAS
Identificación de Eventos					
40. ¿Las Instalaciones donde se encuentra todo el equipo para el funcionamiento Informático de la Organización se encuentra seguro?	✓			**Es adecuado el lugar**	✓
41. ¿Existe personal responsable de la Seguridad de la Organización?	✓				✓ 
42. La salida de Emergencia puede abrirse por ambos lados:		✓		**Solo se abre desde adentro**	*
43. ¿Existen medidas para evitar incendios en la Organización?	✓			**Los empleados tienen prohibido fumar en las Instalaciones, evita la utilización de productos inflamables y se monitorea las conexiones eléctricas**	✓ 
44. ¿En cuanto a las operaciones, se encuentran interconectadas las Terminales?	✓				✓
Evaluación de Riesgos					
45. ¿Las instalaciones son adecuadas para el centro de Cómputo y cómo se encuentran?	✓			**Los espacios para el trabajo se encuentran remodeladas**	✓
46. Los extintores son en base de:			✓	**Polvo/ Espuma**	✓
47. ¿El material emitido por los extinguidores con su uso no hace más daño que el mismo incendio?	✓				✓ 
48. ¿Los Servidores en la Organización se encuentran debidamente protegidos?	✓				✓ 

CUESTIONARIO	SI	NO	N/A	OBSERVACION	MARCAS
Respuesta al Riesgo					
49. ¿Se realizan copias o respaldos en lugares distintos de la Computadora?	✓				✓ 
50. ¿Existen alarmas dentro de la Organización? ¿Cuáles son estas?	✓			**Las alarmas que posee son: Contra Fuego, Contra Robo, Alarma en la Entrada**	✓
51. ¿En la Organización cuentan con extintores?	✓			**Manuales**	✓
52. ¿El personal de la organización sabe cómo manipular los extintores en casos trágicos?	✓				✓
53. ¿La Organización cuenta con Reguladores de voltaje los cuales evitan subidas o bajadas eléctricas?	✓				✓
Actividades de Control					
54. ¿Existe seguridad en la entrada al laboratorio de cómputo y cuál es?	✓			**Se ingresa a través de las llaves entregadas al Personal de Sistemas de la Organización**	✓
55. ¿Posee alarmas la organización y dónde se encuentran ubicadas?	✓			**Contra Fuego: En el espacio de los Clientes y en lugar exclusivo de los empleados Contra Robo: en los cajeros, Alarma en la Entrada: en la puerta secundaria la cual se conecta con la a Empresa de vigilancia**	✓ 
56. ¿Si existiera un incendio, saben los operadores de Sistemas el correcto proceder?		✓		**La empresa cuenta con manual de contingencias pero no se ha comunicado**	* 

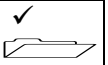
CUESTIONARIO	SI	NO	N/A	OBSERVACION	MARCAS
57. ¿Los extintores se encuentran en constante monitoreo por su proveedor?	✓			**El Cuerpo de Bomberos los monitorea**	✓
58. ¿Se realiza una identificación de los Usuarios?		✓		**La identificación de los Usuarios se las realiza pocas veces**	* 
Información y Comunicación					
59. ¿Se Registra el Acceso al Departamento de Sistemas de parte de personas ajenas al Departamento?		✓		**Existe bitácora de registro pero pocas veces se lo registra**	* 
60. ¿Las alarmas son audibles?	✓				✓
Monitoreo					
61. ¿El Departamento posee medidas de Seguridad?	✓			**Cámaras de Vigilancia y registros escritos de entrada y salida de personal**	✓ 
62. ¿La salida de Emergencia se encuentra en constante monitoreo para evitar posibles catástrofes?	✓			**El Conserje se encarga del mantenimiento**	✓

c) Tecnologías de la Información y Comunicación (Administrador de Sistemas)

CUESTIONARIO	SI	NO	N/A	OBSERVACION	MARCAS
Ambiente Interno					
1. ¿La organización utiliza Internet?	✓				✓
2. ¿La organización utiliza la Intranet?		✓			*
Establecimiento de Objetivos					
3. ¿La Organización cuenta con página Web?	✓				✓
Identificación de Eventos					
4. ¿Para la comunicación entre empleados, lo realiza a través del Correo Electrónico y cuáles son sus características?	✓			**Que es Genérico y además es Personalizado**	✓
Evaluación de Riesgos					
5. ¿La Velocidad de Internet es buena para las labores de la organización y como se encuentra distribuida?		✓		**2 Mb de bajada 1 Mb de subida**	✓
6. ¿Cuenta con distribución de Internet y como se encuentra?	✓			**A través de la conexión cableada a todas las terminales y por medio de WI- FI para el backup.**	✓
Respuesta al Riesgo					
7. ¿Si existiese algún fallo o daño en el servicio de Internet, el proveedor lo soluciona ágilmente?	✓				✓
Actividades de Control					
8. ¿Los correos electrónicos de los socios se encuentran enlistados e ingresados?	✓				✓
Información y Comunicación					
9. ¿La organización cuenta con un proveedor de internet y se llama?	✓			**Telconet / Puntonet**	✓
10. ¿Se utiliza tecnología VOIP para la comunicación?		✓		**Usa los medios Tradicionales**	*
Monitoreo					
11. ¿Se encuentra actualizada la Pagina Web?	✓				✓
12. ¿La Página Web permite a los socios brindarles servicios?	✓				✓

d) Gestión informática (Administrador de Sistemas)

CUESTIONARIO	SI	NO	N/A	OBSERVACION	MARCAS
Ambiente Interno					
32. ¿Para la identificación de puestos clave se encuentran debidamente definidas las funciones?	✓				✓
33. ¿La organización cuenta con un Sistema el cual permita la recolección de Datos?	✓				✓
34. ¿Dentro del manual existen los Procedimientos adecuados con las explicaciones correspondientes?	✓			**Todos los procesos cuentan con explicación**	✓
35. ¿Cuenta con Políticas de Seguridad en la Organización?	✓				✓
Establecimiento de Objetivos					
36. ¿La Organización cuenta con procedimientos Formales los que permita una correcta operación?	✓				✓
37. ¿Las Políticas de Seguridad se encuentran alineadas a las Políticas de la Organización?	✓				✓
38. ¿Las Políticas de Seguridad se encuentran alineadas a las Políticas Legales?	✓				✓
39. ¿Las Políticas de Seguridad se encuentran en un lenguaje el cual sea entendido por todos los empleados de la Organización?	✓				✓
Identificación de Eventos					
40. ¿Posee la debida actualización de los procedimientos?	✓			**Cuando se presente alguna Actualización de equipos**	✓
41. ¿Existe algún mecanismo para la ejecución de programas no autorizados?	✓			**El antivirus evita ejecutarlos**	✓
42. ¿Tiene disponible algún Tipo de Seguro en el equipo?, ¿Cómo se Llama?		✓		**Empresa por contratar, Latina Seguros, un año de vigencia**	*

CUESTIONARIO	SI	NO	N/A	OBSERVACION	MARCAS
Evaluación de Riesgos					
43. ¿En el Caso de que el Sistema Falle, dentro del manual se encuentra el procedimiento para contrarrestarlo?		✓			* 
44. ¿Dentro del registro se muestra el tiempo de congelación de las operaciones, si es mantenimiento o instalación de software?	✓				✓ 
45. ¿Las Políticas de Seguridad son aplicadas por todos los empleados?		✓			* 
Respuesta al Riesgo					
46. ¿Existe un control preventivo para evitar errores y cómo se procede?		✓		**Se revisa solo cuando existe el error después se realiza búsqueda y detección de y se procede a la realización de Documentos si fuere necesario**	* 
47. ¿Cundo existe alguna interrupción en el Sistema, se cuenta con procedimientos escritos para su operación?		✓		**Dentro del manual de procedimientos no se encuentra**	* 
48. ¿Se realiza intervenciones oportunas en los equipos?	✓			**Cuando sea necesario**	✓ 
49. ¿Dispone de alguna Bitácora la que permite llevar el registro del sistema o equipo de cómputo?	✓				✓ 
50. ¿Cuándo la Información almacenada se considera inservible, que procede?	✓			**Se la destruye**	✓  

CUESTIONARIO	SI	NO	N/A	OBSERVACION	MARCAS
Actividades de Control					
51. ¿En los procesos que se genera en el computador existe un control el cual justifique su operación?	✓			**Los procesos se encuentran dentro del manual correspondiente**	✓
52. ¿Realizan revisiones periódicas a los sistemas para determinar si cumplen con los objetivos para los cuales fueron instalados?	✓				✓
53. ¿Cuenta con algún control para la realización de las actividades?	✓			**Por medio de la Utilización de Bitácoras**	✓
54. ¿Tiene un Control por el trabajo realizado fuera del Horario establecido en la Organización?	✓				✓
55. ¿Se realiza la comunicación de las Políticas de Seguridad?		✓			*
56. ¿Existe en la empresa un responsable encargados del desarrollo, revisión y evaluación de la Política de Seguridad con la suficiente formación y experiencia?		✓			*
Información y Comunicación					
57. ¿Cuentan con un mantenimiento periódico, preventivo y correctivo en equipos que lo necesiten?		✓			*
58. ¿Cómo se encuentra organizado el archivo Bitácora?	✓			**Fecha, Hora, Actividad, Responsable**	✓
59. ¿La Organización cuenta con Departamento de Auditoria Interna?	✓				✓
Monitoreo					
60. ¿El operador tiene prohibido la modificación de los archivos?	✓				✓
61. ¿Cuenta con un Inventario Actualizado el cual conste los Equipos, Terminales, y responsables?	✓				✓
62. ¿El Departamento de Auditoria Interna se mantiene Informada y conoce los Aspectos de Sistemas?	✓				✓

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020

ANEXO D: Cuestionario aplicado

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

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

1) ¿Con que frecuencia Ud. cambian las claves de acceso al sistema y/o equipo?

( ) Mensual ( ) Trimestral ( ) Semestral ( ) Anual ( ) Nunca

2) ¿Conoce Usted las medidas de seguridad física implementadas por el área de sistemas del COAC??

Si ( ) No ( )

3) ¿Conoce usted si existen políticas para la seguridad para proteger al sistema informáticos de COAC?

Si ( ) No ( )

4) ¿A su criterio el equipo informático que usted utiliza le ayuda a cumplir sus actividades laborales en una forma:

( ) Excelente ( ) Bueno ( ) Regular ( ) Malo

5) ¿Las condiciones eléctricas para el funcionamiento de del sistema informático del COAC considera usted que son?:

( ) Excelente ( ) Bueno ( ) Regular ( ) Malo

6) ¿El Sistema Informático que utiliza actualmente el COAC para el manejo de la Información, es:

( ) Excelente ( ) Bueno ( ) Regular ( ) Malo

7) ¿Conoce usted si existe un plan de mantenimientos para los equipos informáticos del COAC?

( ) Bastante ( ) Poco ( ) Nada

8) ¿Existe una comunicación previa cuando va existir cambios que los equipos informáticos?

Si ( ) No ( )

9) ¿La información que Ud. generar en el sistema informáticos del COAC lo guarda en?

( ) Propia PC ( ) Disco externo ( ) Unidades de almacenamiento ( ) Nube

10) ¿Conoce usted si se ha socializado el plan de contingencia del COAC en caso de algún Tipo de Riesgo?

Si ( ) No ( )

GRACIAS POR SU COLABORACIÓN

Fuente: Desarrollo de la Investigación

Realizado por: Merizalde Guamanzara, Paúl Alejandro, 2020