ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

CARRERA INFORMÁTICA

TESIS PREVIA LA OBTENCIÓN DEL TÍTULO DE

INGENIERAS EN INFORMÁTICA

TEMA:

AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA A LOS RECURSOS DE TECNOLOGÍA DE INFORMACIÓN EN LA CARRERA INFORMÁTICA DE LA ESPAM MFL

AUTORAS:

AMARILIS CAROLINA LOOR PÁRRAGA

VERÓNICA ALEXANDRA ESPINOZA CASTILLO

TUTOR:

ING. SERGIO ANTONIO INTRIAGO BRIONES, MS.C.

CALCETA, MARZO 2014

DERECHOS DE AUTORÍA

Espinoza Castillo Verónica Alexandra y Loor Párraga Amarilis Carolina, declaran bajo juramento que el trabajo aquí descrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido por la Ley de Propiedad Intelectual y su reglamento.

…… ……..……

VERÓNICA A. ESPINOZA CASTILLO **AMARILIS C. LOOR PÁRRAGA**

CERTIFICACIÓN DE TUTOR

Sergio Antonio Intriago Briones certifica haber tutelado la tesis **AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA A LOS RECURSOS DE TECNOLOGÍA DE INFORMACIÓN EN LA CARRERA INFORMÁTICA DE LA ESPAM MFL**, que ha sido desarrollada por Verónica Alexandra Espinoza Castillo y Amarilis Carolina Loor Párraga, previa la obtención del título de Ingeniera Informática, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

……..……..

ING. SERGIO A. INTRIAGO BRIONES MS.C

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaran que han **APROBADO** la tesis **AUDITORÍA DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS RECURSOS DE TECNOLOGÍAS DE INFORMACIÓN DE LA CARRERA INFORMÁTICA**, que ha sido propuesta, desarrollada y sustentada por Verónica Alexandra Espinoza Castillo y Amarilis Carolina Loor Párraga, previa la obtención del título de Ingeniera Informática, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

..... **.....**

ING. JESSICA J. MORALES CARRILLO
MIEMBRO

DRA. MARÍA I. MATILLA BLANCO
MIEMBRO

.....

ING. GUSTAVO G. MOLINA GARZÓN
PRESIDENTE

AGRADECIMIENTO

A la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López que nos dio la oportunidad de una educación superior de calidad y en la cual hemos forjado nuestros conocimientos profesionales día a día;

A nuestros padres, madres, hermanos y nuestras familias por el apoyo incondicional que nos demuestran en cada una de nuestras etapas de vida.

A los y las docentes de la carrera de Informática, que mediante sus conocimientos impartidos, nos guían hacia nuestra vida profesional.

A nuestros amigos y amigas de clases, por consolidarnos en verdadera amistad compartiendo duras y hermosas luchas de superación.

Y a todas aquellas personas que directa o indirectamente nos han demostrado su compromiso de solidaridad y estima.

LAS AUTORAS

DEDICATORIA

Con mi infinito amor dedico este trabajo investigativo:

A mi mamá, Vitalia Párraga Zambrano, mujer que amo y que me demuestra a luchar por mis metas y la que me da a conocer el rostro tierno y servicial de la vida.

A mi papá Rafael Loor Basurto, hombre que admiro y que me enseña que con esfuerzo y sacrificio se pueden culminar los proyectos, él me demuestra el rostro trabajador de la vida.

A mi hermano Rolando Loor Párraga, al que respeto y que con su toque amigable y fraterno me mostró el rostro alegre y rebelde de la vida.

A toda mi familia, que muchas veces me ayudaron en la ejecución de varios proyectos.

AMARILIS C. LOOR PÁRRAGA

DEDICATORIA

Con mi gran amor dedico este trabajo investigativo:

A mis padres por ser el pilar fundamental en todo lo que soy, en toda mi educación, tanto académica, como de la vida, por su incondicional apoyo perfectamente mantenido a través del tiempo.

A mi familia en general, porque me han brindado su apoyo incondicional y por compartir conmigo buenos y malos momentos.

VERÓNICA A. ESPINOZA CASTILLO

CONTENIDO

CONTENIDO DE CUADROS Y FIGURAS

RESUMEN

La auditoría de seguridad física y lógica aplicada en la Carrera Informática, de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, permitió evaluar la integridad de los recursos de tecnologías de información existentes en la entidad, para el efecto, se empleó la metodología determinada en las Normas Internacionales de Auditoría, dividida en tres fases: Planificación, incluyó un análisis integral de todos los elementos internos y externos a la entidad, empleando la evaluación de control interno con la finalidad de determinar los eventos de mayor relevancia, en la fase de Ejecución se aplicaron los programas de auditoría, los que permitieron evidenciar los principales hallazgos suscitados en la entidad, y en la fase de Comunicación de Resultados se describieron las conclusiones y recomendaciones mediante la presentación del Informe Final. En base a los resultados obtenidos de la evaluación de control interno, se determina que la entidad auditada aplica lineamientos generales de seguridad, situación que se comprueba con el Coeficiente de Concordancia de Kendall, evidenciando que el grado de coincidencia equivale a 0,85, por lo que se concluye que la Carrera Informática, cuenta con un bajo control documentado de procedimientos aprobados, por lo tanto, es conveniente la aplicación de normativas de seguridad que permitan tomar mayor responsabilidad, minimizando posibles riesgos en la infraestructura tecnológica.

PALABRAS CLAVES

Auditoría, Seguridad Física, Seguridad Lógica, Recursos de Tecnología.

ABSTRACT

This research aims to evaluate the safety of existing resources information technology in the Computer Science of the Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, an audit of physical and logical security is performed between October 2013 and February 2014, for the purpose, the methodology established on the Auditing International Standards which is divided into three phases, the first one corresponds to the Planning and includes a comprehensive analysis of all the elements involved in the entity, complemented by the evaluation of internal control of regulation that is issued by the Controller General of the State, the second is the Execution where audit programs for components are applied and determined to be assessed, such as data integrity among others, in this section, there are evident the main findings raised in the entity. Finally, the Communication Result phase, where are described the conclusions and recommendations through presenting the Final Audit Report. With the results of the evaluation of internal control, it is determined that the audited entity applies general safety guidelines, a situation that is checked to obtain the Kendall concordance coefficient of 0.85, and the evaluated entity has a documented control of approved procedures, therefore recommended developing control regulations such as Security Policy, among others.

KEY WORDS

Audit, Physical Security, Logic Segurity, Technology Resources.

CAPÍTULO I. ANTECEDENTES

1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

A nivel mundial la auditoría informática constituye un pilar fundamental en las organizaciones, porque tanto los sistemas como las estructuras físicas deben estar sometidos a controles de calidad. En la actualidad este enfoque es necesario para poder alertar a los empresarios de la importancia que tiene la protección de sus equipos de cómputo, para prevenir o evitar daños físicos.

En la encuesta de Global Securtity Survey 2013, elaborada por la Empresa Deloitte, determina que en Europa lo que más motiva a realizar auditorías informáticas en las organizaciones, está relacionado con el cumplimiento de normativas vigentes, que proporcionen controles de calidad en la entidad. Sin embargo, en Latinoamérica lo que hace que se realice este tipo de auditorías, está vinculado con la adopción de mejores prácticas que certifiquen que los procesos se están llevando conforme a lo que establece la ley.

Por ello, considerando que la Carrera Informática de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López ESPAM MFL, cuenta con importantes recursos tecnológicos, que pueden ser víctimas de amenazas, pudiendo ocasionar pérdidas económicas a la institución, por lo que, resulta conveniente mantener mecanismos de seguridad sobre ellos.

Según lo expuesto, la auditoría sobre la seguridad física y lógica, permitirá determinar el nivel de riesgo y el grado de confianza que mantienen los recursos tecnológicos de la Carrera Informática, respecto a los controles de seguridad que se están utilizando, con el fin de incrementar la confiabilidad en los procesos y reducir los riesgos.

En virtud a lo manifestado, las autoras se plantean la siguiente interrogante:

¿Cómo evaluar la seguridad física y lógica de los recursos de tecnología de información de la Carrera Informática de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López de la ciudad de Calceta?

1.2. JUSTIFICACIÓN

La confiabilidad de la información tiene cada vez mayor importancia en la sociedad, puesto que se enfoca en la protección de los datos, en la infraestructura computacional y todo lo relacionado con esta (Granados, 2012). Es así que la auditoría informática se constituye en una herramienta que gestiona la tecnología de la información en las entidades (Ramírez y Álvarez, 2008) normadas en una serie de estándares, leyes, manuales, reglas, controles concebidas nacional o internacionalmente para minimizar los posibles riesgos de seguridad de estos recursos.

La ejecución de una tesis de auditoría, permitirá una evaluación objetiva de la seguridad de los recursos tecnológicos y así fortalecer sus conocimientos y dar cumplimiento a la Ley Orgánica de Educación Superior (LOES, 2010) en lo establecido en el Art. 8 literal h que textualmente expresa: “Contribuir con el desarrollo local y nacional de manera permanente, a través del trabajo comunitario o extensión universitaria”, de esta manera se da un aporte a la investigación en temas relacionados con auditorías informáticas.

Es imprescindible que al abordar este tema en una tesis de investigación, se ha de tomar en cuenta el Art. 9 de la (Ley Orgánica de la Contraloría General del Estado, 2002) que indica literalmente que: El control interno constituye un proceso aplicado por la máxima autoridad, la dirección y el personal de cada institución, que proporciona la seguridad razonable de que se protegen los recursos públicos y se alcancen los objetivos institucionales.

Conjuntamente, la Ley de Transparencia de Información Pública (LOTAIP, 2004), declara en el Art.- 1. “Principio de Publicidad de la Información Pública.- El acceso a la información pública es un derecho de las personas que garantiza

el Estado. Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público… las organizaciones de trabajadores y servidores de las instituciones del Estado, instituciones de educación superior que perciban rentas del Estado, las denominadas organizaciones no gubernamentales (ONGs), están sometidas al principio de publicidad; por lo tanto, toda información que posean es pública, salvo las excepciones establecidas en esta Ley".

Además, la LOTAIP declara en el Art.- 5. Información Pública.- Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado.

Con referencia a lo anterior, resulta conveniente realizar una auditoría de la seguridad física y lógica de los recursos de tecnologías de información de la Carrera Informática de la ESPAM MFL, con la finalidad de evaluar el estado actual de los mismos, identificando los posibles riesgos, recomendando acciones de mejoras para el manejo y seguridad de equipos e información, salvaguardando de esta manera equipos públicos y poder seguir con el desarrollo educativo consagrado en los objetivos de la Carrera.

Es así que, evaluar la seguridad de los recursos de las tecnologías de información no solo logra la protección de estos, sino que también, se salvaguarda la integridad física de las personas que desarrollan sus actividades laborales y académicas en las diferentes áreas de la institución, reduciendo así, costos económicos para la institución y para las personas.

Y conociendo que la Carrera Informática de la ESPAM MFL es consciente que los procesos que se llevan a cabo son importantes para la institución y que la protección de los recursos tecnológicos es imprescindible, las autoras justifican el tema ya mencionado, mediante las fases de auditoría que se basan en normas y estándares nacionales e internacionales.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Aplicar una auditoría de seguridad física y lógica a los recursos de tecnologías de información en la Carrera Informática, de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López de la ciudad de Calceta, evaluando la integridad de los mismos.

1.3.2. OBJETIVOS ESPECÍFICOS

- ✓ Comprobar la existencia de elementos que brinden salvaguarda a la infraestructura física de la carrera.

- ✓ Identificar controles de tecnologías de información.

- ✓ Verificar el nivel de cumplimiento de las políticas, planes y procedimientos que emplea la Carrera de Informática en cuanto al uso de los recursos tecnológicos.

- ✓ Evaluar vulnerabilidades ante una interrupción del servicio.

- ✓ Elaborar el Informe de Auditoría en la seguridad física y lógica considerando todos los hallazgos encontrados.

1.4. IDEA A DEFENDER

La aplicación de una auditoría de la seguridad física y lógica en la Carrera de Informática de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López de la ciudad de Calceta, permitirá evaluar los recursos de tecnologías de información de la misma.

CAPÍTULO II. MARCO TEÓRICO

2.1. AUDITORÍA

La auditoría es un examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado, con frecuencia este término ha sido utilizado incorrectamente, ya que se ha considerado como una evaluación donde el fin es detectar errores y señalar fallas, pero el concepto de auditoría va más allá de la detección de errores, es un examen crítico donde el objetivo es evaluar la eficiencia y la eficacia de un área u organismo (Martínez, 2012).

La auditoría es un proceso sistemático para obtener y evaluar de manera objetiva, las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados, cuyo fin consiste en determinar el grado de correspondencia del contenido con las evidencias que le dieron origen, así como establecer si dichos informe se han elaborado observando los principios establecidos para el caso (Martínez *et al.,* 2012).

Con lo mencionado anteriormente, las autoras definen como auditoría al proceso sistemático de evaluación de las actividades que se ejecutan en una entidad determinada, mediante el uso de técnicas y herramientas acopladas a la realidad del negocio.

2.1.1. LA AUDITORÍA INTERNA

Hernández (2010) manifiesta que la auditoría interna es una actividad que tiene por objetivo fundamental examinar y evaluar la adecuada y eficaz aplicación de los sistemas de control interno, velando por la preservación de la integridad del patrimonio de una entidad y la eficiencia de su gestión económica, proponiendo a la dirección las acciones correctivas pertinentes.

2.1.2. LA AUDITORÍA EXTERNA

La auditoría externa es aquella que es realizada por una firma externa de profesionales con el propósito de examinar y evaluar cualquiera de los sistemas de información de una organización. Se trata de un procedimiento de uso común cuando se quiere comprobar que una empresa se maneja de forma honrosa. Se suele recurrir a las auditorías externas por ser agentes externos a la empresa y así poder tener un criterio más objetivo (González, 2009).

2.1.3. AUDITORÍA INFORMÁTICA

La auditoría informática como técnica y herramienta de apoyo a la organización, ha facilitado en las últimas décadas el desarrollo en el área de sistemas, debido al auge que han tenido en estos últimos años.

La labor de la auditoría informática trata de cuestionar la fiabilidad de los equipos que albergan información, comienza entonces a plantearse nuevos objetivos de control, como el control de acceso sobre la información, la gestión de autorizaciones, quién puede acceder a qué información, qué puede hacer con ella o a cuestionar de la integridad de las misma, y los mecanismos de registro de actividad sobre la información (Pons, 2007).

Según Piattini *et al*., (2008) la auditoría informática también conocida como auditoría de sistemas de información es la revisión y la evaluación de los controles, de sistemas, procedimientos de informática, de los equipos de cómputo, su utilización, eficiencia y seguridad de la organización, que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

En concordancia con Piattini *et al*., (2008), las autoras consideran que la auditoría informática es un proceso que consiste en almacenar, verificar y evaluar evidencias para determinar si un sistema de información salvaguarda el

patrimonio de la entidad, manteniendo la integridad y confidencialidad de los datos.

2.1.3.1. SEGURIDAD INFORMÁTICA

La seguridad informática concierne a la protección de la información, que se encuentra en una computadora o en una red de ellas y también a la protección del acceso a todos los recursos del sistema (Baldeón, 2012).

Para ello, se deben evaluar y cuantificar los bienes a proteger, y en función de análisis, implantar medidas preventivas y correctivas que eliminen los riegos asociados o que los reduzcan hasta niveles manejables (Morlanes, 2012).

La seguridad debe ser apropiada y proporcionada al valor de los sistemas, al grado de dependencia de la organización a sus servicios y a la probabilidad y dimensión de los daños potenciales. Los requerimientos de seguridad variarán por tanto, dependiendo de cada organización y de cada sistema en particular (Castro, 2009).

Las manifestaciones de incidentes, ha creado un estado de situación en materia de seguridad informática, que exige que los usuarios de diferentes herramientas informáticas, instituciones gubernamentales y no gubernamentales, conozcan y utilicen principios y normas que les permitan evitar, saber y actuar frente a los incidentes de seguridad más frecuentes. Para ello debe desplegar iniciativas de superación con personal de diferentes entidades, con el objetivo de que las mismas, cuenten con personas preparadas para difundir y preparar a distintos usuarios de las TI, en materia de normas y buenas prácticas en seguridad Informática (Rodríguez, 2010).

Por consiguiente, las autoras concretan que la seguridad informática consiste en asegurar que las actividades que se ejecutan en la entidad, garantizan la protección, la integridad y la privacidad de la información almacenada en un sistema informático.

2.1.3.1.1. GESTIÓN DEL RIESGO

Según Ramos, (2002) la protección de los sistemas y de la información no suele eliminar completamente la posibilidad de que estos bienes sufran daños. En consecuencia, los gestores deben implantar aquellas medidas de seguridad que lleven los riesgos hasta niveles aceptables, contando para ello con el coste de las medidas a implantar, con el valor de los bienes a proteger y con la cuantificación de las pérdidas que podrían derivarse de la aparición de determinado incidente de seguridad.

Para la SEDISI (2002) el riesgo es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema de información, causando un impacto en la empresa. Hoy los responsables de la tecnología deben estar más orientados a la administración de riesgos operacionales, debido a que éste puede afectar de manera positiva o negativa la gobernabilidad corporativa y las operaciones diarias del negocio.

En cualquier caso, la seguridad informática exige habilidad para gestionar los riesgos de forma adecuada. Invirtiendo en medidas de seguridad, las organizaciones pueden reducir la frecuencia y la severidad de las pérdidas relacionadas con violaciones de la seguridad en sus sistemas (Bernal, 2006).

2.1.3.1.2. AMENAZAS

Es la causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización (Carrasco, 2013).

La seguridad informática se ha convertido en punto crítico de las comunicaciones realizadas a través de Internet, debido al gran número de amenazas contra los datos expuestos al viajar a través de este medio. Estas amenazas se presentan en distintas formas, tienen como propósito causar el mayor daño posible a la información almacenada en los sistemas. Las principales amenazas son: los virus informáticos, los gusanos de Internet, el

spyware, caballos de Troya, el pharming, el pshishing scam, ataques de negación de servicio, entre otros (Jiménez, 2008).

Los efectos de las diversas amenazas puedes ser muy variados. Unos pueden comprometer la integridad de la información o de los sistemas, otros pueden degradar la disponibilidad de los servicios y otros pueden estar relacionados con la confidencialidad de la información. En cualquier caso una correcta gestión de los riesgos debe implicar un profundo conocimiento de las vulnerabilidades de los sistemas y de las amenazas que los pueden explotar (Hernández, s.f.).

Las propias características de las organizaciones deben influir en las medidas de seguridad que resulten más adecuadas y más eficientes en términos de costes, para contrarrestar las amenazas o incluso para tolerarlas conociendo en todo caso sus implicaciones (Davara, 2004).

2.1.3.1.3. MEDIDAS DE SEGURIDAD

Existe un gran abanico de medidas de seguridad que pueden reducir el riesgo de pérdidas debidas a la aparición de incidentes en los sistemas informáticos. Muchas veces al hablar de medidas de seguridad, solo se mencionan las meramente técnicas, como cortafuegos, antivirus o sistemas de copias de respaldo. (Galdámez, 2003) Sin embargo, las medidas más efectivas suelen ser las medidas de gestión planteadas a medio y largo plazo desde un punto de vista estratégico y táctico (James, 2008).

2.1.3.1.4. .MEDIDAS DE GESTIÓN

Los gestores de toda organización deberían contemplar la seguridad informática como parte integral de las estrategias y tácticas corporativas. Una vez plasmada la importancia de los sistemas para la consecución de los propios objetivos y los riesgos que puede suponer para la empresa la pérdida de integridad de su información, la indisponibilidad de sus sistemas o la

violación de la confidencialidad de su información, pueden plantearse con mayor rigor el resto de medidas encaminadas a servir a los objetivos empresariales (Morant y Sancho, 2009).

Las políticas de seguridad de una organización son las normas y procedimientos internos que deben seguir los integrantes de la organización para respetar los requerimientos de seguridad que deseen preservarse. Debe describirse la criticidad de los sistemas y de la información, los roles de cada puesto de trabajo y la mecánica de acceso a los sistemas, herramientas, documentación y cualquier otra componente del sistema de información (Galdámez, 2003).

Resulta frecuente desglosar las políticas de seguridad en procedimientos detallados para cada componente del sistema de forma individualizada, así por ejemplo, pueden crearse documentos que describan las políticas de tratamiento de correos electrónicos, políticas de uso de Internet, de copias de respaldo, de tratamiento de virus y otra lógica maliciosa, políticas normativas en materia de seguridad, entre otros. Conviene destacar que las políticas de seguridad deben emanar de la estrategia corporativa y que se trata de documentos que deberían conocer todos los integrantes de la plantilla (Day, 2003).

2.1.3.1.5. MEDIDAS TÉCNICAS

Entre las técnicas más consolidadas encontramos las copias de respaldo, los antivirus, los cortafuegos, los mecanismos de autenticación y la criptografía. Las copias de respaldo y en general cualquier forma de redundancia, se encaminan a garantizar la disponibilidad de los sistemas frente a cualquier eventualidad (Romero, 2012).

Los antivirus pretenden evitar la aparición de lógica maliciosa y en caso de infección tratan de eliminarla de los sistemas. Entre los antivirus conviene destacar aquellos que inspeccionan los correos electrónicos evitando la

infección de sus destinatarios. Por su parte, los cortafuegos tratan de reducir el número de vías potenciales de acceso a los sistemas corporativos desde el exterior, estableciendo limitaciones al número de equipos y de servicios visibles. Otra de las técnicas imprescindibles en toda organización la forman los mecanismos de autenticación (Donaire, 2011).

Estos mecanismos pueden variar desde esquemas simples basados en los pares usuario contraseña, hasta complejos sistemas distribuidos establecidos en credenciales o sistemas de autenticación biométricos con reconocimiento mecanizado de características físicas de las personas. Por último, todo esquema de seguridad debe contemplar en una u otra medida el cifrado de información sensible. A veces puede ser suficiente cifrar las contraseñas, mientras que en otras resulta imprescindible el cifrado de las comunicaciones y de las bases de datos.

Como medidas más avanzadas, podemos mencionar la esteganografía, la detección de vulnerabilidades y la detección de intrusos. Las técnicas esteganográficas tratan de ocultar información. A diferencia de la criptografía, que trata de hacer indescifrable la información, la esteganografía trata de evitar que siquiera se note su existencia (Barchini, *et al*., s.f.).

2.1.3.2. TIPOS DE AUDITORÍA INFORMÁTICA

Lamere (2009) sustenta que la auditoría informática tiene varios tipos, entre los cuales se citan a continuación:

2.1.3.2.1. AUDITORÍA OFIMÁTICA

Comprende los programas o aplicaciones que en conjunto sirven de herramienta para generar, procesar, almacenar, recuperar, comunicar y presentar la información en un lugar de trabajo, así como de forma doméstica.

2.1.3.2.2. AUDITORÍA DE BASE DE DATOS

Es el proceso que permite medir, asegurar, demostrar, monitorear y registrar los accesos a la información almacenada en las bases de datos incluyendo la capacidad de determinar: quién accede a los datos, cuándo se accedió a los datos, desde qué tipo de dispositivo/aplicación, desde que ubicación en la red, cuál fue el efecto del acceso a la base de datos, entre otros.

2.1.3.2.3. AUDITORÍA DE REDES

Se encarga de una serie de mecanismos mediante los cuales se pone a prueba una red informática, evaluando su desempeño y seguridad, a fin de lograr una utilización más eficiente y segura de la información. En primer instancia una gestión responsable de la seguridad es identificar la estructura física (hardware, topología) y lógica (software, aplicaciones) del sistema, y hacerle un análisis de vulnerabilidad para saber en qué grado de exposición se encuentra la entidad de esta manera estudiada la "radiografía" de la red, se procede a localizar sus falencias más críticas, para proponer una estrategia de saneamiento de los mismos; un plan de contención ante posibles incidentes y un seguimiento continuo del desempeño del sistema.

2.1.3.2.4. AUDITORÍA DE LA SEGURIDAD

En concordancia con Piattini *et al*. (2008) la seguridad es el área principal a auditar, hasta el punto de que en algunas entidades se creó inicialmente la función de auditoría informática para revisar la seguridad, la importancia de la información, especialmente relacionada con sistemas basados en el uso de tecnología de información y comunicaciones, por lo que el impacto de las fallas, los accesos no autorizados, la revelación de la información, entre otros problemas, tienen un impacto mucho mayor.

De este modo este tipo de auditoría sustenta y confirma la consecución de los objetivos tradicionales de la auditoría:

- Objetivos de protección de activos e integridad de datos.

- Objetivos de gestión que abarcan, no solamente los de protección de activos, sino también los de eficacia y eficiencia (SEDISI, 2007).

El auditor evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informáticos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso del software.

En muchos casos, ya no es posible verificar manualmente los procedimientos informatizados que resumen, calculan y clasifican datos, por lo que deberá emplear software de auditoría y otras técnicas por ordenador.

El auditor es responsable de revisar e informar a la dirección de la organización sobre el diseño y el funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada.

El estudio de la seguridad tradicionalmente se suele dividir en dos grandes bloques: Seguridad Lógica y Seguridad Física (Fitzgerald, 2003).

- **AUDITORÍA DE LA SEGURIDAD FÍSICA**

En la seguridad física es conocido el grave impacto que los desastres naturales tienen sobre las infraestructuras de todo tipo, de las que los sistemas informáticos forman parte, y de las que así mismo dependen para su adecuado funcionamiento.

Hoy en día, la línea que separa estos dos bloques entre la seguridad física y seguridad lógica, es cada vez más difusa, debido sobre todo a que los elementos de las salvaguardas técnicas se utilizan tanto para proteger activos de carácter físico como lógico (Ramírez, 2012).

Las cuatro normas de la seguridad física son: evitar, retrasar, detectar y defender, siendo estas de aplicación a la protección física de los sistemas de información (Lamere, 2009).

Concordando con las definiciones anteriores, la auditoría en seguridad física, es aquella actividad que controla, verifica, califica, supervisa, analiza y recomienda, sobre el estado actual de seguridad en sus instalaciones e infraestructura, sean estas empresariales, industriales, o de cualquier otra naturaleza.

- **AUDITORÍA DE LA SEGURIDAD LÓGICA**

Una auditoría de seguridad lógica se centra en auditar aspectos técnicos de la infraestructura de Tecnología de Información y Comunicación (TIC), contemplando tantos diseños de la arquitectura desde el punto de vista de seguridad, como aspectos relacionados con los mecanismos de protección desplegados para hacer frente a todo tipo de incidentes lógicos.

La auditoría informática cuando examina la seguridad lógica verifica que existan los procedimientos necesarios para controlar todos los componentes y que las configuraciones de cada componente no permiten que se puedan acceder sin conocimiento de la gestión de TIC (Castilla, 2007).

Una auditoría más profunda, pasa a la revisión de permisos específicos asignados por usuario, de tal forma que se establezca que no existen accesos y privilegios asignados adicionales a los necesarios para cumplir con su perfil de trabajo. Incluso se puede llegar a utilizar herramientas de “hackeo ético”, para lograr probar que la infraestructura lógica está bien configurada y no está dejando vulnerabilidades expuestas.

Este análisis realizado por la auditoría informática provee a la alta dirección un nivel adicional de garantía, de que la seguridad lógica está siendo bien administrada (Piattini *et al*., 2008).

En consecuencia a lo manifestado, las autoras definen como auditoría a la seguridad lógica el proceso mediante el cual se controla y verifica aquellos accesos que han sido diseñados para salvaguardar la integridad de la información almacenada en diferentes medios.

2.1.3.1. PROCESO DE LA AUDITORÍA INFORMÁTICA

Según Hervada (2007) el proceso de la auditoría informática es un examen crítico pero no mecánico, que no implica la preexistencia de fallas en la entidad auditada y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo. La auditoría contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones, la revisión analítica a la suficiencia de controles establecidos en el ámbito informático, con la finalidad de disminuir los riesgos y garantizar la seguridad, confiabilidad y exactitud de la información.

De acuerdo a las Normas Internacionales de Auditoría, el proceso de la auditoría comprende las siguientes fases (IAASB, 2009).

2.1.3.1.1. PLANEACIÓN DE LA AUDITORÍA

Su objetivo es obtener un conocimiento de la entidad u organización sobre cómo operan los sistemas de información que se han de incluir en la revisión y el ambiente de control en cuanto a las fuentes de información, evaluación de riesgos inherentes al control e identificación de controles claves, para definir el enfoque de auditoria que se aplicará, determinar los procedimientos de auditoria específicos a realizar, seleccionar al personal, determinar tiempo y costo y preparar los programas de auditoría respectivos (Navarro, 2005).

Según Martínez *et, al.* (2012). Define las siguientes etapas en la planeación de la auditoría:

- **REVISIÓN PRELIMINAR**

Viloria (2009), manifiesta que la revisión preliminar consiste en obtener información necesaria para que el auditor pueda tomar la decisión de cómo proceder en la auditoría, significa la recolección de evidencias por medio de entrevistas con el personal de la entidad, la observación de las actividades y la revisión de la documentación preliminar.

Al terminar la revisión preliminar el auditor puede proceder a seguir una de las tres opciones:

- Diseñar la auditoría.
- Realizar una revisión detallada de los controles internos.
- Decidir no confiar en los controles internos.

- **REVISIÓN ESPECÍFICA**

Consiste en obtener la información necesaria para que él o la auditor/a tenga un profundo entendimiento de los controles usados dentro del área de informática. En esta fase es importante para el auditor identificar las causas de las pérdidas existentes dentro de la instalación y los controles para reducir las pérdidas y los efectos causados por esta (Dussan, 2008).

- **PROGRAMACIÓN DE LA AUDITORÍA**

El Plan de Auditoría debe estar basado en la comprensión de las actividades de las entidades, sus sistemas de administración y control, la naturaleza de las transacciones que realiza y las leyes y reglamentos que le aplican. Debe ser documentado como parte integral de los papeles de trabajo y modificado, cuando sea necesario durante el transcurso de la auditoria.

La planeación es imprescindible para todo tipo de trabajo, cualquiera sea su tamaño. Sin una adecuada planeación es prácticamente imposible obtener efectividad y eficiencia en la ejecución de los trabajos, debe ser cuidadosa y

creativa, positiva e imaginativa y tener en cuenta alternativas para realizar las tareas, seleccionando lo métodos más apropiados, es decir, determinando un enfoque de auditoría adecuado y práctico, acorde con las circunstancias (Ramos. 2005).

- **COMPRENSIÓN DEL CONTROL INTERNO**

Se debe comprender y evaluar el control interno para identificar las áreas críticas que requieren un examen profundo y determinar su grado de confiabilidad a fin de establecer la naturaleza, alcance y oportunidad de los procedimientos de auditoría a aplicar.

Existen dos tipos de controles: el control general y el control detallado de los sistemas de información. El control general involucra a todos los sistemas de información y el control detallado está diseñado para controlar el procesamiento en sí de la información (Pinket, 2006).

- **DESARROLLO DE LA ESTRATEGIA DE AUDITORÍA**

En función de la naturaleza, complejidad y del objeto de auditoría, se determinarán las áreas críticas, dependiendo de éstas se definirán los objetivos o el(los) enfoque(s) y el alcance de la auditoria.

El Plan Estratégico de una auditoria de sistemas representa el soporte sobre el cual estarán basadas todas las actividades requeridas para la ejecución del trabajo y para alcanzarlo de forma eficiente (Maldonado, 2008).

- **COMPRENSIÓN DE LA ENTIDAD Y DE SUS AMBIENTE**

Al planificar una auditoría, el auditor informático debe tener una comprensión suficiente del ambiente total que revisará. Este conocimiento debe incluir una comprensión general de las diversas prácticas y funciones de la auditoría, así

como los tipos de sistemas de información que se utilizan. También, debe comprender el ambiente normativo del negocio (Muñoz, 2008).

Los pasos que puede llevar a cabo un auditor informático para obtener una comprensión de la entidad pueden incluir:

- Recorrer las instalaciones de la organización
- Lectura material sobre antecedentes que incluyan publicaciones sobre memorias, informes financieros independientes
- Entrevista con gerentes claves para comprender los temas
- Estudios de los informes
- Informes de auditorías previas y planes estratégicos, entre otros.

➢ RIESGO Y MATERIALIDAD DE AUDITORÍA

Se tiene que definir los riesgos de la auditoría como el riesgo de que la información pueda contener errores materiales o de que el auditor Informático pueda no detectar un error que no ha ocurrido. Pueden clasificar los riesgos de auditoría de la siguiente manera:

1.1. Riesgo de Control: Es el riesgo de que existe un error importante que no se ha detectado ni evitado oportunamente por el sistema de control interno.

1.2. Riesgo de Detección: Riesgo de que un auditor use un procedimiento inadecuado de pruebas y concluye que no existen errores importantes, cuando en realidad si existen.

1.3. Riesgo Inherente: Es la susceptibilidad de que en una actividad existan errores o irregularidades significativos, antes de considerar la efectividad de los sistemas de control.

1.4. Riesgo Residual: Es el riesgo restante después de evaluar la eficiencia de los controles o características mitigantes del ambiente en que opera.

1.5. Riesgo Retenido: Es el nivel de riesgo con el cual decido vivir, después de la evaluación de los controles mitigantes.

Cabe señalar que la materialidad exige al auditor de SI un juicio claro, basado en que para el auditor Informático es más complicado la materialidad (Mandarriaga, 2006).

- **PROGRAMA DE AUDITORÍA**

Se deberán efectuar programas a la medida que incluyan las listas de procedimientos de auditorías para examinar los sistemas, tanto a nivel de Controles Generales del Computador como Controles Generales de Aplicación.

Los Programas de Auditoría detallados son los instrumentos metodológicos mediante los cuales se pone en ejecución la “Planeación General de la Auditoría” documentada en el Memorando de Planeación y su preparación es responsabilidad del Auditor de Sistemas, el cual llega ser la guía a los auditores para ejecutar los procedimientos y proporciona un registro permanente de la auditoria para facilitar la supervisión final.

Las áreas o aspectos a evaluar en una auditoría de sistemas son: la planeación de las aplicaciones, el inventario de sistemas en proceso, la situación de cada aplicación (Cepeda, 2008).

2.1.3.1.2. EJECUCIÓN DE LA AUDITORÍA INFORMÁTICA

Esta etapa de la auditoría consiste en el desarrollo de los procedimientos contenidos en los programas de auditoría a través de técnicas de auditoría. Es la estructuración de un proceso uniforme para el desarrollo de las auditorías, en

el cual las actividades están principalmente enfocadas a identificar riesgos de TI y evaluar la calidad de los controles para la gestión de los riesgos.

Las alternativas de solución que puede adoptar el Administrador, son reconocidas como controles/monitoreo, las cuales pueden circunscribirse a: evitar, reducir, compartir o aceptar los riesgos. Se concreta con la aplicación de los programas elaborados en la planificación específica y el cumplimiento de los estándares definidos en el Plan de la Auditoría (Armas, 2006).

- **HALLAZGOS DE AUDITORÍA**

El término hallazgo se refiere a debilidades en el control interno detectadas por el auditor. Por lo tanto, abarca los hechos y otras informaciones obtenidas que merecen ser comunicados a los funcionarios de la entidad auditada y a otras personas interesadas.

Los hallazgos en la auditoría, se definen como asuntos que llaman la atención del auditor y que en su opinión, deben comunicarse a la entidad, ya que representan deficiencias importantes que podrían afectar en forma negativa, su capacidad para registrar, procesar, resumir y reportar información confiable y consistente, en relación con las aseveraciones efectuadas por la administración (Whitten, 2008).

- **ELEMENTOS DEL HALLAZGO DE AUDITORÍA**

Según Piattini (2008) desarrollar en forma completa todos los elementos del hallazgo en una auditoría, no siempre podría ser posible. Por lo tanto, el auditor debe utilizar su buen juicio y criterio profesional para decidir cómo informar determinada debilidad importante identificada en el control interno. La extensión mínima de cada hallazgo de auditoría dependerá de cómo éste debe ser informado, aunque por lo menos, el auditor debe identificar los siguientes elementos:

- **Condición:** Se refiere a la situación actual encontrada por el auditor al examinar un área, actividad, función u operación, entendida como “lo que es”.

- **Criterio:** Comprende la concepción de “lo que debe ser “, con lo cual el auditor mide la condición del hecho o situación.
- **Efecto:** Es el resultado adverso o potencial de la condición encontrada, generalmente representa la pérdida en términos monetarios originados por el incumplimiento para el logro de la meta, fines y objetivos institucionales.

- **Causa:** Es la razón básica (o las razones) por lo cual ocurrió la condición, o también el motivo del incumplimiento del criterio de la norma. Su identificación requiere de la habilidad y el buen juicio del auditor y, es indispensable para el desarrollo de una recomendación constructiva que prevenga la recurrencia de la condición.

- **EVIDENCIAS DE AUDITORÍA**

La evidencia de auditoría es el conjunto de hechos comprobados, suficientes, competentes y pertinentes (relevantes) que sustentan las conclusiones de auditoría. Las evidencias de auditoría constituyen los elementos de prueba que obtiene el auditor sobre los hechos que examina y cuando éstas son suficientes y competentes, constituyen el respaldo del examen que sustenta el contenido de la auditoría (Govindan, 2007).

Indica la obligatoriedad de obtener evidencia suficiente, competente y pertinente” para sustentar los hallazgos de auditoría.

- **PAPELES DE TRABAJO**

Según Razo (2008) los papeles de trabajo de una auditoría de sistemas constituyen el sustento del trabajo llevado a cabo por el auditor especialista, así

como de los comentarios, conclusiones y recomendaciones incluidos en su informe, representado por la evidencia en ellos contenida.

La organización de centros de cómputos, seguridad de los sistemas de control y prácticas de control, la administración de los sistemas de información, los procesos mismos de datos, la integridad, confiabilidad, confidencialidad y disponibilidad que brindan los sistemas computacionales, el desarrollo, adquisición y mantenimiento de los sistemas son tópicos y casi seguro de la importancia para el control de los registros que soporta la cifras y controles de cualquier reporte importante para una entidad, en su sentido amplio, constituyen un conjunto de aseveraciones o declaraciones formuladas por la administración en torno a los resultados de su gestión.

Los papeles de trabajo de la auditoría deberán mostrar los detalles de la evidencia, la forma de su obtención, las pruebas a que fue sometido y las conclusiones sobre su validez. Son propiedad absoluta del auditor condicionando su uso únicamente a los propósitos de su revisión y soporte de los resultados obtenidos.

- **TÉCNICAS DE AUDITORÍA**

De acuerdo con Piattini *et, al.* (2008) para la obtención de evidencias se pueden utilizar diversos tipos de técnicas, procedimientos y herramientas de auditoría, de los cuales destacan el análisis de datos, debido que para las organizaciones el conjunto de datos o información son de tal importancia, por lo que es necesario verificarlos y comprobarlos; utilizando diversas técnicas para el análisis de datos, entre las cuales los autores nombran las siguientes:

- **CUESTIONARIOS**

El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Se envían cuestionarios preimpresos a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar. Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma.
Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría. Se recomienda solo hacer preguntas necesarias, que permitan alcanzar el objetivo; preguntas sencillas y directas, no hacerlas abiertas, porque dificultan el análisis.

- **ENTREVISTAS**

El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:

- Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.
- Mediante entrevistas en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.
- Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

Para el caso del auditor informático, siempre tienen que ser su entrevista preparada y con preguntas sistematizadas, que en un ambiente de cordialidad

le permita al usuario dar la información que el auditor requiere, de una manera sencilla.

- **CHECKLIST**

Además del chequeo de los sistemas, el auditor somete al auditado a una serie de cuestionario. Dichos cuestionarios, llamadas Check List, tienen que ser comprendidas por el auditor al pie de la letra, ya que si son mal aplicadas y mal recitadas se puede llegar a obtener resultados distintos a los esperados.

La Check List puede llegar a explicar cómo ocurren los hechos pero no por qué ocurren. El cuestionario debe estar subordinado a la regla, a la norma, al método.

El profesionalismo para utilizar las checklist, pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente. Salvo excepciones, las Checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

- **MATRIZ DE RIESGO**

Una matriz de riesgo es una herramienta de control y de gestión normalmente utilizada para identificar las actividades (procesos y productos) más importantes de una institución, el tipo y nivel de riesgos inherentes a estas actividades y los factores exógenos y endógenos que engendran estos riesgos (factores de riesgo). Igualmente, una matriz de riesgo permite evaluar la efectividad de una adecuada gestión y administración de los riesgos financieros, operativos y estratégicos que impactan la misión de la organización.

- **PRUEBAS DE CUMPLIMIENTO**

El objetivo de la Prueba de Cumplimiento es determinar si el control interno es adecuado y si está funcionando en la forma que se planeó en el área de informática. Las Pruebas de Cumplimiento deben apoyarse en el alcance que se determinó, pudiendo soportarlo a través de: (Villar de francos y Rivera, 2008).

- Documentación.
- Manuales de usuario, técnicos y procedimientos.
- Cambios en los programas.
- Solicitud por escrito.
- Pruebas por parte de los usuarios.
- Actualización de los manuales técnicos y de usuarios
- Verificar que los cambios en los programas sean realizados por el personal de informática o por el proveedor de la aplicación.
- Copias de respaldo y recuperaciones.
- Contenidos de las copias.
- Periodicidad de las copias.
- Persona responsable.
- Custodia, almacenamiento, inventario, rotación de la cinta.
- Acceso a datos y programas.
- Verificar la lista de usuarios que tiene acceso.
- Revisar el procedimiento para otorgar y eliminar los accesos.
- Analizar la periodicidad de los cambios de los passwords (clave).
- Capacitación de los usuarios
- Controles en la entrada, proceso y salida

2.1.3.1.3. COMUNICACIÓN DE RESULTADOS

En concordancia con lo que estable Contraloría General del Estado en su acuerdo 26-CG-2012, esta etapa tiene por objetivo efectuar el cierre del

proceso de auditoría, confeccionando el Informe de Auditoría a partir de los resultados y conclusiones obtenidas en las evaluaciones y pruebas desarrolladas en la etapa anterior e incorporándolos planes de acción de los responsables. Es importante destacar que una auditoría puede dar origen a investigaciones especiales o auditorías específicas. En conclusión general la auditoría realizada en el informe debe contener:

- Objetivos de auditoría cubiertos.
- Naturaleza y alcance de los procedimientos aplicados.
- Hallazgos detectados y recomendaciones de auditoría.
- Comentarios de los funcionarios de la entidad u organismos.
- Conclusiones.

Siendo el Informe el documento formal, y el producto final de la auditoria de SI, en el cual se establecen la naturaleza, alcance y resultados de nuestros procedimientos de auditoria, su importancia es fundamental, pues resulta ser el documento que le interesa a la entidad auditada. El Informe de Auditoría deberá comprender:

1. Carta de envío
2. Información introductoria.

2.1. Motivo, objetivos y alcance de la auditoria.

2.2. Un breve resumen de los resultados de auditoria, control interno, cumplimiento con las leyes y regulaciones aplicables, y estado de las recomendaciones anteriores.

3. Informe de Auditoría informática que debe contener:

3.1. Resultados de auditoría que expondrán los hallazgos significativos que tengan relación con los objetivos de auditoría, los que incluirán la información suficiente que permita una adecuada comprensión del asunto que se informa.

3.2. Las conclusiones, que son inferencias lógicas sobre el objeto de auditorías basadas en los hallazgos.

2.2. PRINCIPIOS ÉTICOS DEL AUDITOR INFORMÁTICO

Según Muñoz (2002) los principios son un conjunto de preceptos que establecen los deberes exigibles a aquellos profesionales que ejerciten una determinada actividad, tienen como finalidad incidir en sus comportamientos profesionales estimulando que éstos se ajusten a determinados principios morales que deben serviles de guía, entre los principales el autor cita los siguientes:

- **Comportamiento Profesional:** El auditor debe actuar conforme a las normas de dignidad de la profesión y de corrección en el trato personal y evitar caer en exageraciones innecesarias, transmitiendo una imagen de precisión y exactitud en sus comentarios.

- **Confianza:** Consiste en facilitar e incrementar la confianza del auditado en base a una actuación transparente en su actividad profesional, aceptar las indicaciones del auditado como válidas (excepto contradicciones), disponer de diálogo por ambas partes para aclarar dudas sobre aspectos conflictivos que pudieran surgir así como un buen lenguaje al nivel de comprensión del auditado.

- **Discreción:** Consiste en la divulgación de los datos, especialmente cuando dichos datos pudieran afectar a la intimidad o profesionalidad de las personas concernidas por los mismos o a intereses empresariales.

- **Integridad Moral:** Obligación del auditor a ser honesto, leal y diligente en el desempeño de su misión, ajustarse a las normas de justicia y evitar participar en actos de corrupción personal o de terceras personas no utilizar los conocimientos adquiridos durante la auditoría en contra del auditado o de terceras personas.

- **Secreto Profesional:** No difundir a terceras personas ningún dato que haya visto, oído o deducido durante el desarrollo de su trabajo que

pudiera perjudicar a su cliente, siendo nulos cualquier pacto contractual que pretendieran excluir dicha obligación, establecimiento de medidas y mecanismos de seguridad para garantizar al auditado que la información documentada va a quedar almacenada en entornos o soportes que impidan la accesibilidad a la misma por terceras personas no autorizadas.

2.3. COEFICIENTE DE CONCORDANCIA DE KENDALL

El coeficiente de concordancia de Kendall, al que la mayoría de los autores simboliza por la letra W, es una técnica de análisis estadístico muy utilizado en medición del grado de concordancia entre un grupo de elementos y un grupo de características.

Si la concordancia es la máxima posible. W=1, el máximo valor que puede tener el coeficiente W es la unidad; por el contrario, si la concordancia es la mínima posible, es decir no hay concordancia W = 0. Por lo tanto el coeficiente puede oscilar entre 0 y 1 (Álvarez, 1995).

CAPÍTULO III. DESARROLLO METODOLÓGICO

El presente trabajo de investigación realizado en la Carrera Informática de la ESPAM MFL en la ciudad de Calceta, tuvo la duración de seis meses. Para el inicio de la auditoría de seguridad física y lógica de los recursos tecnológicos de información, fue necesario solicitar la autorización de inicio (**Anexo 1)** a la máxima autoridad, el ingeniero Leonardo Félix López, Rector de la Politécnica de Manabí, la misma que describía aspectos como los objetivos de auditoría, el alcance, personal involucrado y el tiempo estimado, obteniendo así el respectivo permiso.

Para el desarrollo del trabajo, se utilizó la metodología de auditoría, basada en las Normas Internacionales de Auditoría, emitidas por el Consejo de Normas Internacionales y Aseguramiento IAASB órgano encargado de la emisión de las mismas, con el objetivo de promover la calidad y la uniformidad de la práctica a nivel mundial. Esta metodología se dividió en tres fases: planificación, ejecución y comunicación de los resultados de la auditoría, mediante las cuales, las autoras llevaron a cabo la aplicación del trabajo.

Esta metodología a su vez se convirtió en una herramienta de apoyo, permitiendo incorporar el uso de la Norma Técnica ISO 27001 referente a Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la Información y la Norma de Control Interno 410, referente a Tecnología de Información, la misma que está dirigida para las entidades y organismos del sector público del Ecuador, sirviendo de guía para el desarrollo del Plan de Auditoría y del Programa de Auditoría.

3.1. FASE I. PLANIFICACIÓN DE LA AUDITORÍA

Para llevar a cabo una planificación estructurada en el desarrollo de la auditoría, las autoras realizaron el Plan de Auditoría (**Anexo 2**) con el propósito de definir los objetivos, asignar los recursos, talento humano y estimar el

tiempo necesario en el que se iba a efectuar la revisión, con la finalidad de fijar un orden para la ejecución de la misma.

La fase de planificación se dividió en dos subfases, denominados planificación preliminar y planificación específica. En la primera de ellas, se configuró en forma preliminar la estrategia a seguir en el trabajo, a base del conocimiento acumulado e información obtenida en la Carrera Informática; mientras que en la segunda se definió tal estrategia mediante la determinación de los procedimientos específicos a aplicarse por cada uno de los componentes y la forma en que se desarrolló el trabajo.

3.1.1. PLANIFICACIÓN PRELIMINAR

Mediante esta etapa las auditoras se familiarizaron con el entorno de la entidad, observando de forma más directa las áreas a evaluar, con el objeto de obtener la información necesaria de los factores relevantes. Es por ello, que en esta fase se definió el Programa de Auditoría Preliminar (**Anexo 3**), el mismo que promueve el eficiente manejo del trabajo, el talento humano y permite el logro efectivo de sus objetivos.

Esta fase se inició con la aplicación de cuestionarios de control interno preliminares (**Anexo 4**), los mismos que permitieron obtener una idea global de las actividades y operaciones, así como la identificación de políticas y prácticas administrativas que se llevan a cabo en la Carrera Informática.

Por consiguiente, uno de los puntos importantes para la recopilación de la información, estuvo basado en la preparación y aplicación de técnicas de auditoría como son las entrevistas y reuniones con el personal involucrado en la auditoría, para comunicarles sobre la ejecución del trabajo e identificar, datos, hechos e información relevante.

Posteriormente, para fortalecer el conocimiento sobre el entorno de la Carrera Informática, se realizaron visitas a las instalaciones del edificio, para obtener

información general de las actividades y procesos ejecutados. Por lo tanto, fue importante contar con la información proporcionada por la entidad, debido a que esto permitió evaluar en forma profesional el medio en el cual desarrollan sus operaciones, logrando identificar de manera preliminar las áreas de mayor riesgo, a fin de asegurar que dichos aspectos reciban una especial atención.

Una vez que se concluyó con la planificación preliminar, fue necesario elaborar el Memorando de Planificación Preliminar (**Anexo 5**), con el propósito de dar a conocer los resultados obtenidos en esta fase, dicho memorando está conformado por los antecedentes, el motivo de la auditoría, los objetivos de la auditoría, el alcance de la auditoría, conocimiento de la entidad, puntos de interés para la planificación específica y los componentes a ser examinados.

En términos generales, esta etapa incluyó un análisis integral de todos los elementos internos y externos a la entidad, con la finalidad de determinar los eventos con la mayor relevancia para cumplir con la misión y objetivos estratégicos de la Carrera Informática.

3.1.2. PLANIFICACIÓN ESPECÍFICA

Los productos obtenidos en la planificación preliminar fueron el pilar fundamental para definir los procedimientos a cumplir en la planificación específica, para lo cual, esta fase inicia con la preparación del Programa Específico de Auditoría (**Anexo 6**), el cual incluye entre sus elementos los programas de auditoría por componentes.

Es así, que para la recopilación de datos específicos se aplicó una evaluación de control interno enfocada a las áreas involucradas en la auditoría, tal como lo expresan las Normas de Control Interno, dicha evaluación se ejecutó a través de cuestionarios de control interno, como se demuestra en el capítulo de resultados.

En relación a lo anterior, los cuestionarios cerrados dicotómicos están compuestos por una serie de preguntas objetivas diseñadas en una matriz, que tienen por objetivo medir el nivel de cumplimiento de los procesos, por lo tanto, estos se encuentran estructurados de la siguiente manera: poseen una ponderación de diez puntos por cada pregunta; y la calificación asignada está basada dentro de un rango de puntación (0 – 10), donde, 0 representa que dicho proceso no se cumple, 5 determina que el proceso se cumple en un 50% y 10 establece que los procedimientos se cumple en su totalidad, es decir en un 100%, dicho rango de puntuación está fundamentado en el criterio de las auditoras, en base a las respuestas y evidencias obtenidas por parte de los entrevistados.

Sin embargo, para que tal información posea soporte sustentable, se solicitó documentación a las áreas involucradas en la auditoria. Para tal efecto, una vez aplicados los cuestionario de control interno, se procedió a elaborar la matriz de determinación del riesgo - confianza; la misma que inicia con la siguiente fórmula definida en el Manual General de Auditoría (CGE, 2003).

$$\mathrm{CP} = \frac{\mathrm{CT} * 100}{\mathrm{PT}} \qquad \textbf{(3.1)}$$

CP: Calificación Porcentual
PT: Ponderación Total
CT: Calificación Total

Para obtener la calificación porcentual (CP), se multiplicó la calificación total (CT) por 100 y se dividió para la ponderación total (PT).

La calificación porcentual, permitió identificar el grado de confianza y nivel de riesgo por cada componente examinado, asignando un tipo de color en cada nivel, de acuerdo a la siguiente tabla de calificación.

Cuadro 3.1. Determinación del Nivel de Confianza y del Riesgo.

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLORES
15 – 50	BAJO	ALTO	ROJO
51 – 75	MODERADO	MODERADO	AMARILLO
76 - 95	ALTO	BAJO	VERDE

Fuente: Contraloría General del Estado, 2003.

El cuadro 3.1. determina el nivel de confianza y riesgo, está divido en tres columnas, en la de calificación porcentual se describe la escala que inicia con el 15% porque no existe empresa totalmente sin control, y termina con el 95% porque no hay empresa con control total eficiente y efectivo debido a que toda entidad está sujeta a un mejoramiento continuo.

En la columna de grado de confianza se detalla el nivel, que puede ser bajo, moderado o alto, estos registros son proporcionales al nivel de riesgo, definidos en la tercera columna y puede ser, alto, moderado o bajo.

Los resultados que se obtuvieron en esta etapa, se presentaron en una matriz, con la finalidad de determinar su nivel de riesgo y confianza, por lo cual, aquellos controles que resultaron con efectividad inapropiada generaron una o más observaciones.

Es así, que para la comprensión de los resultados se elaboró un cuadro resumen de los resultados porcentuales obtenidos de la evaluación de control interno por cada componente examinado, evidenciado en el capítulo de resultados.

Para la comprobación de datos que concuerdan en los cuestionarios, se clasificaron 4 preguntas en común, analizadas mediante el Coeficiente de Concordancia de Kendall (*w)*, que ofrece el valor que posibilita establecer el nivel de concordancia entre los encuestados.

Según la evidencia obtenida por las autoras, la comprobación se llevó a cabo evaluando la respuesta de cada persona, de acuerdo a las preguntas de los cuestionarios, clasificando cada respuesta en base a su cumplimiento de 1 a 4, es decir, se asigna la puntuación de 1 para el parámetro que tenga mayor cumplimiento, y así correspondientemente hasta 4, número que le pertenece al que tenga menor cumplimiento.

El valor que determina *w* oscila entre 0 y 1. Si el valor de w es ≥ a 0,5 significa gran concordancia entre los encuestados y si el valor de w es < a 0,5 denota un desacuerdo total, por lo tanto los datos no son confiables. Dichos valores surgen de la siguiente fórmula propuesta por Kendall (Pérez, 2007).

$$w = \frac{12\sum A^2}{n^2\, n(k^2-1)} \qquad \textbf{(3.2)}$$

Dónde:

k=Números de preguntas

n=Número de personas entrevistadas

$\sum A^2$= Suma de ponderaciones

Para determinar el valor de A, se aplica la siguiente fórmula:

$$A = \sum aij - T \qquad \textbf{(3.3)}$$

Dónde:

$\sum aij$= Suma de puntuación

T= Factor de comparación

Para establecer el valor de T, se aplicó la siguiente fórmula:

$$T = \frac{\sum aij}{k} \qquad \textbf{(3.4)}$$

Obtenidos los resultados del Coeficiente de Concordancia de Kendall y concluida la evaluación de control interno se procedió a la elaboración del Memorando de Planificación Específica (**Anexo 7**), el mismo que resume los

aspectos más significativos de la planificación de auditoría, que incluye elementos como los antecedentes de la planificación preliminar y resultados de la evaluación de control interno.

3.2. FASE II. EJECUCIÓN DE LA AUDITORÍA

Con la información que se obtuvo en la primera fase y luego de tener conocimiento de los procesos que se llevan a cabo, las autoras procedieron a aplicar los Programas de Auditoria por componentes (**Anexo 8**), con el objetivo de planificar y determinar la extensión de las pruebas de cumplimiento, las mismas que evalúan los controles y verifican si estos operan de forma adecuada y dan cumplimiento a los objetivos de la Carrera Informática.

Para lo cual, se aplicaron pruebas de cumplimiento a aquellos controles que una vez identificados y evaluados, están operando como se previó, por tal motivo, estas pruebas tuvieron como objetivo comprobar (obtener evidencia) que los controles establecidos están implantados y que las personas encargadas de las operaciones los entienden, ejecutan y supervisan.

El propósito de esta fase fue identificar y documentar los controles existentes por cada proceso que se lleva en la entidad auditada, a su vez, el soporte del levantamiento de esta información, fue la descripción narrativa de las actividades que se ejecutan en la entidad y con la información recopilada, se procedió a evaluar la satisfacción de los objetivos de control ya identificados en esta etapa.

Las observaciones de auditoría se registraron en hojas de hallazgos y se analizaron describiendo la desviación identificada, respecto a las actividades observadas. Posteriormente, se detalló el impacto o perjuicios, a los que se expone la organización como consecuencia de la deficiencia o debilidad del control identificado.

Es así, que se determina si los controles establecidos en los procesos de la Carrera Informática, ofrecen la protección apropiada para reducir los riesgos a niveles aceptables. Esto es, evaluar la confiabilidad de los controles utilizados para prevenir o detectar y corregir las causas de los riesgos y minimizar el impacto que estos tendrían en caso de llegar a materializarse.

En el desarrollo de una auditoría, la evaluación del cumplimiento de las leyes y reglamentos es de fundamental importancia debido a que los organismos, programas, servicios, actividades y funciones se rigen generalmente por las leyes, ordenanzas, decretos y están sujetas a disposiciones legales y reglamentarias específicas.

3.3. FASE III COMUNICACIÓN DE RESULTADOS

Esta es la última fase de la auditoría, en ella se resumieron los resultados más significativos obtenidos en las etapas anteriores. Estos fueron los insumos para elaborar el Informe de Auditoría (**Anexo 9**), con el cual se comunicó al director de la Carrera Informática y a los demás interesados, las observaciones, conclusiones y recomendaciones sobre las características de seguridad, calidad y confiabilidad de la información y de los recursos tecnológicos y humanos que intervienen en las actividades de control de los procesos de negocio y sistemas de información.

El Informe de Auditoría es un documento formal, que tiene como objetivo comunicar las observaciones encontradas, suscitar la respuesta con las acciones de mejoramiento para solucionar los problemas detectados. El informe consta de las siguientes tres secciones: a) Objetivos y alcance de la auditoría: Los objetivos y el alcance se encuentran descritos en el plan de auditoría, también, se hizo énfasis en el período de tiempo que cubrió la revisión y el rango de las fechas durante las cuales se efectuó la auditoría; b) Antecedentes generales: Este capítulo contiene una breve descripción de las características y atributos del área auditada, con la finalidad de ubicar a los interesados dentro de un marco de referencia que le ayude a comprender el

informe y la importancia de las observaciones de la auditoría; c) Observaciones de la auditoría: Esta parte del informe presenta, para cada proceso y sistema evaluado, las observaciones y debilidades de control identificados por la auditoría.

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

En el presente capítulo, se detallan los resultados de los procesos realizados en cada fase de la Auditoría Física y Lógica de los recursos de tecnología de información, los mismos que se describen a continuación:

En la fase de planificación se elaboró el Plan de Auditoría, el cual estableció el enfoque general del trabajo.

Debido a que la planificación se divide en dos subfases como lo es la planificación preliminar y la planificación específica, en la primera etapa las autoras elaboraron el Programa de Planificación Preliminar, el mismo que definió las directrices a seguir, comenzando así con la aplicación de cuestionarios de control interno preliminares, cuyos resultados permitieron obtener información acerca del entorno en el que se desenvuelve la Carrera Informática, dicha información es mostrada en el Memorando de Planificación Preliminar.

Lo realizado en la planificación preliminar fue elemental para definir los procedimientos a ejecutarse en la planificación específica, al igual que en la parte preliminar, en esta etapa se elabora el Programa de Planificación Específica, que definen las acciones a seguir, iniciando con la elaboración de los Programas de Auditoría por componentes**,** y posteriormente la evaluación de control interno, cuyo resultados se muestran en el Memorando de Planificación Específica.

A continuación se muestran los resultados obtenidos mediante la aplicación de los cuestionarios de control interno, los mismos que dan cumplimiento a los objetivos de la auditoría, estos fueron aplicados a las áreas de Dirección de Carrera, Desarrollo de Software, Mantenimiento y Soporte Técnico, Centro de Datos, Redes.

Cuadro 4.1. Cuestionario de Control Interno aplicado al Data Center.

CARRERA INFORMÁTICA DE LA ESPAM MFL

CUESTIONARIOS DE CONTROL INTERNO

Componente: Seguridad Data Center

ÁREA AUDITADA: Data Center	**FECHA DE APLICACIÓN:**
DIRIGIDO A: Ing. César Moreira	**FUNCIÓN:** Administrador del Data Center

N°	PREGUNTAS	RESPUESTA		CUMPLIMIENTO		OBSERVACIONES
		SI	NO	POND	CAL	
1	¿Existe una política de seguridad, para la administración del Data Center?	X		10	5	Desarrolladas por el administrador, pero no están documentadas. Las mismas quedarán para el Data Center.
2	¿Están descritas sus funciones y responsabilidades?	X		10	5	
3	¿Todas las políticas de seguridad que se utilizan cuentan con el respaldo de las autoridades?	X		10	5	Las autoridades conocen de las políticas a raíz de una conversación.
4	¿Están identificados y documentados los riesgos a los que está expuesto el Data Center?	X		10	5	Se han identificado y comunicado informalmente, no están documentados.
5	¿El Data Center tiene inventariados sus activos?	X		10	5	Reposan en el departamento de Almacén de

						la ESPAM MFL.
6	¿El Data Center cuenta con mecanismos de acceso de seguridad?	**X**		**10**	5	Sistema de biometría y llaves, sin embargo la puerta sólo está cerrada con seguro en su ausencia.
7	¿Está definido quienes son las personas autorizadas para el acceso al Data Center?	**X**		**10**	10	Administrador, el Director de Carrera y la persona que realiza limpieza.
8	¿Están controlados las visitas y el acceso de personas no autorizadas al Data Center?	**X**		**10**	10	El ingreso es solo de estudiantes de la carrera y docentes para hacer prácticas, con la supervisión del Administrador del Centro de Datos.
9	¿Existe un registro de las personas que ingresan al Data Center?	**X**		**10**	5	En la base de datos del biométrico, pero no de los visitantes.
10	¿Existe un programa que controle el estado y funcionamiento de los equipos del Data Center?		**X**	**10**	0	Los procesos realizados son por procesos redundantes, se monitorea los paquetes.
11	¿Posee Racks y Gabinetes para organizar los componentes del Data Center?	**X**		**10**	10	
12	¿Está el cableado de datos debidamente canalizado y rotulado?	**X**		**10**	10	Norma internacional de cableado estructurado.
13	¿Se utiliza piso falso para la distribución de cableado de datos y/o electricidad?	**X**		**10**	5	Se ha perforado y se visibilizan las últimas instalaciones como las cámaras.

14	¿Se efectúa limpieza periódica en los pisos falsos?	**X**		**10**	5	Al ser nueva la edificación aún no se ha realizado.
15	¿Existen procedimientos de asignación y distribución de usuarios y contraseñas?	**X**		**10**	5	La solicitud es informal ante el administrador del data center, no existe un formato establecido.
16	¿Se eliminan las cuentas de usuarios del personal que ya no forma parte de la carrera?	**X**		**10**	10	Expiración automática de la clave, y en el correo se inhabilita.
17	¿El sistema de autenticación de usuarios guarda las contraseñas encriptadas?	**X**		**10**	10	
18	¿Existe un sistema de bloqueo de cuentas por el intento de acceso con claves erróneas?	**X**		**10**	5	Para el acceso a la red, con tres intentos fallidos y se bloquea a nivel de navegador, no existe bloqueo en el servidor.
19	¿Están restringidos los horarios de conexión de los usuarios y las usuarias?		**X**	**10**	0	
20	¿Se han documentado procedimientos de acción y salida del recurso tecnológico en caso de una emergencia en el Data Center?	**X**		**10**	5	La información se replica entre 18 y 20 horas, para los equipos no los hay, no existe un atrapa rayos.
21	¿Existen medios de vigilancia interna y/o externa en el Data Center?	**X**		**10**	10	Guardias del edificio y las cámaras. Existen ventanas en el área.

22	¿El Data Center cuenta con un segmento de red exclusivo para la ejecución de sus operaciones?	**X**		**10**	10	Y se cuenta con un DMZ servidor de balanceo de carga.
23	¿Se ha establecido medios para el almacenamiento y respaldo de información?	**X**		**10**	10	Las replicaciones y el Cloud computing infraestructura de servicios.
24	¿Existen detectores de humo, polvo y/o de humedad?	**X**		**10**	5	No se están habilitados aún, pero los detectores activan el extinguidor de agua, desfavorable para el Data Center.
25	¿Se mantiene la instalación del servidor libre de polvo, humo y de otros materiales, como alimentos?	**X**		**10**	10	La limpieza al área 3 veces a la semana, limpieza a los equipos casi todos los días.
26	¿Cuenta con un sistema de extinción de incendios?	**X**		**10**	5	Extintor no ideal para los equipos.
27	¿Se cuenta con equipos de aire acondicionados que permitan controlar la temperatura de los servidores?	**X**		**10**	10	Mínimo 18 ^{o}C y 24 ^{o}C.
28	¿Está la red equipada con dispositivo de suministro ininterrumpido de alimentación (UPS) que permita a la red operar en casos de fluctuaciones menores de la energía eléctrica o ser apagado debidamente en caso de un corte prolongado de energía?	**X**		**10**	5	Funcionamiento de las UPS (no tienen baterías) por 30 minutos hasta que se restablezca la energía eléctrica, pasado se apagan.

29	¿Se realizan actualizaciones en los sistemas operativos, aplicaciones?		**X**	**10**	0	Existe un SO base independiente, con cambio previsto en 15 años.
30	¿Utiliza Firewalls para la protección de la red interna?	**X**		**10**	10	
31	¿Los servidores en el Data Center cuentan con protección actualizada contra virus informáticos?	**X**		**10**	5	El sistema operativo base Linux de 64 bits.
32	¿Existe un plan de contingencia en caso de desastres?		**X**	**10**	0	
TOTALES		**28**	**4**			
Σ PONDERACIÓN TOTAL (PT)				**320**		
Σ CALIFICACIÓN TOTAL (CT)					**200**	
FIRMA Y SELLO DEL ENTREVISTADO				**FIRMA DEL ENTREVISTADOR**		

Fuente Administrador del Data Center

Cuadro 4.2. Matriz de Riesgo - Confianza del Data Center.

MATRIZ DE RIESGO - CONFIANZA

Determinación del riesgo confianza:

CP: Calificación Porcentual

PT: Ponderación Total

CT: Calificación Total

$$CP = \frac{CT * 100}{PT}$$

$$CP = \frac{200 * 100}{320}$$

$$CP = 62{,}50\ \%$$

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO
15 – 50	BAJO	ALTO
51 – 75	**MODERADO**	**MODERADO**
76 - 95	ALTO	BAJO

62,50%

Nivel de confianza:	**MODERADO**	62,50%
Nivel de riesgo:	**MODERADO**	37,50%

El cuestionario de control interno aplicado al componente Seguridad del Data Center, integrado por 32 preguntas, obtuvo la contestación de 28 respuestas positivas y 4 respuestas negativas; obteniendo la ponderación total de 320 puntos y la calificación total de 200 puntos, lo que representa una calificación porcentual del 62,50%, determinando un nivel de riesgo moderado y a su vez el grado de confianza moderado.

Cuadro 4.3. Cuestionario de Control Interno aplicado a la Protección de Activos Tangibles

CARRERA INFORMÁTICA DE LA ESPAM MFL **CUESTIONARIOS DE CONTROL INTERNO** **Componente:** Protección de Activos Tangibles						
ÁREA AUDITADA: Dirección de Carrera		**FECHA DE APLICACIÓN:**				
DIRIGIDO A: Ing. Luis Cedeño Valarezo		**FUNCIÓN:** Director de Carrera				
N°	**PREGUNTAS**	**RESPUESTA**		**CUMPLIMIENTO**		**OBSERVACIONES**
		SI	**NO**	**POND**	**CAL**	
1	¿Existe una política de seguridad vigente en la Carrera Informática?	**X**		**10**	5	No están documentadas, llevan proceso de control como las cámaras.
2	¿Están descritas sus funciones y responsabilidades?	**X**		**10**	10	
3	¿Se han realizado análisis de riesgo y amenazas en la seguridad de la carrera?		**X**	**10**	0	
4	¿Se han contratado seguros generales para la edificación y recursos de la carrera?		**X**	**10**	0	

5	¿Existe un contrato de seguro que garantice la continuidad del negocio en caso de emergencia?		**X**	**10**	0	
6	¿Existe planos de la edificación de la carrera?	**X**		**10**	10	
7	¿Existe un estudio acerca de la posibilidad de inundación en la zona?		**X**	**10**	0	
8	¿Existen planos de todas la conducciones y están actualizados? (Climatización, agua, energía eléctrica, redes y comunicaciones)	**X**		**10**	5	
9	¿Existen rutas de salida y emergencia?	**X**		**10**	5	Se ha fijado rutas de salidas pero no todas están señalizadas, ni luces emergentes.
10	¿Existen sistemas de vigilancia y seguridad en la edificación y sus aulas y laboratorios?	**X**		**10**	10	
11	¿Existen controles de acceso en la Carrea?	**X**		**10**	5	Se restringe el acceso de personas no autorizadas a los laboratorios oficinas, a la edificación no se controla.

12	¿La ubicación del centro de datos ha sido estudiada y documentada?	**X**		**10**	5	Plano de la carrera, no se ajusta a normas de seguridad puesto que existen ventanas en el área, dispensadores de agua.
13	¿Existe un estudio de las condiciones estructurales del edificio? (Pared, vigas , suelo y techos)	**X**		**10**	5	
14	¿Existe un registro de todos los accesos a las salas de equipos informáticos de la carrera?	**X**		**10**	5	Registro de las autenticaciones en el biométrico, los estudiantes son supervisados por los docentes.
15	¿Existe un sistema de control biométrico a las áreas de la carrera?	**X**		**10**	10	Respaldo de llaves.
16	¿Todas las personas con acceso autorizado tienen un código de identificación y están controlados?	**X**		**10**	10	Biometría.
17	¿Existen procedimientos específicos de control para acceso al personal ajeno a la carrea?	**X**		**10**	5	Sólo a los laboratorios y aulas.

18	¿Se han verificado la resistencia de las ventanas, puertas y calidad de las cerraduras?		**X**	**10**	0	
19	¿Existe un control de entrada y salida de los recursos tecnológicos de la carrera?	**X**		**10**	10	Documentado en actas entrega recepción, para mantenimiento mediante oficio.
20	¿Existe un procedimiento de horario para la realización de la limpieza en los laboratorios y áreas de la carrera?	**X**		**10**	10	
21	¿Existe un sistema automático de detección de incendios y está conectado a una central de alarmas?	**X**		**10**	5	No se detecta en alarma.
22	¿Existe un sistema autónomo de generación de energía?		**X**	**10**	0	
23	¿Están inventariados los recursos tecnológicos de la carrera?	**X**		**10**	10	
24	¿El uso de los recursos de tecnologías de información administrativo, son de uso exclusivo del personal encargado?	**X**		**10**	10	

25	¿El tiempo de uso de los recursos tecnológicos de los laboratorios es de uso exclusivo de la carrera y se usan solo en clases de la carrera de informática?		**X**	**10**	0	
26	¿Está documentado el convenio de prestar los laboratorios?		**X**	**10**	0	CAI
27	¿La entrega y asignación de recursos tecnológicos al personal, es documentada?	**X**		**10**	10	Se documenta en acta entrega
28	¿Se conoce y documenta cuáles son los riesgos a los que están sujetos los recursos tecnológicos de la carrera?	**X**		**10**	5	
29	¿Se ha restringido a los usuarios el consumo de alimentos y bebidas en el interior de laboratorios para evitar daños al equipo?	**X**		**10**	10	
30	¿Está capacitado el personal que labora, sobre el uso y responsabilidad de la custodia del recurso tecnológico?	**X**		**10**	10	
31	¿Se revocan los derechos de acceso al sistema cuando los usuarios finalizan su actividad en la empresa?		**X**	**10**	0	

32	¿Se cuenta con mecanismos que impidan el robo de los recursos tecnológicos de la carrera?	**X**		**10**	10	Cámaras
TOTALES		**23**	**9**			
Σ PONDERACIÓN TOTAL (PT)				**320**		
Σ CALIFICACIÓN TOTAL (CT)					**180**	
FIRMA Y SELLO DEL ENTREVISTADO				**FIRMA DEL ENTREVISTADOR**		

Fuente: Director de la Carrera Informática

Cuadro 4.4. Matriz de Riesgo - Confianza de Protección de Activos Tangibles

MATRIZ DE RIESGO - CONFIANZA

Determinación del riesgo confianza:

CP: Calificación Porcentual

PT: Ponderación Total

CT: Calificación Total

$$CP = \frac{CT * 100}{PT}$$

$$CP = \frac{180 * 100}{320}$$

$$CP = 56,25\%$$

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO
15 – 50	BAJO	ALTO
51 – 75	**MODERADO**	**MODERADO**
76 - 95	ALTO	BAJO

56,25%

Nivel de confianza:	**MODERADO**	56,25%
Nivel de riesgo:	**MODERADO**	43,75%

El cuestionario de control interno aplicado al componente Protección de Activos Tangibles por 32 preguntas, obtuvo la contestación de 23 respuestas positivas y 9 respuestas negativas; obteniendo la ponderación total de 320 puntos y la calificación total de 180 puntos, lo que representa una calificación porcentual del 56,25%, determinando un nivel de riesgo moderado y a su vez el grado de confianza moderado.

Cuadro 4.5. Cuestionario de Control Interno aplicado a la Protección de Activos Intangibles

CARRERA INFORMÁTICA DE LA ESPAM MFL **CUESTIONARIOS DE CONTROL INTERNO** **Componente:** Protección de Activos Intangibles						
ÁREA AUDITADA: Dirección de Carrera		**FECHA DE APLICACIÓN:**				
DIRIGIDO A: Ing. Luis Cedeño Valarezo		**FUNCIÓN:** Director de Carrera				
N°	**PREGUNTAS**	**RESPUESTA**		**CUMPLIMIENTO**		**OBSERVACIONES**
		SI	**NO**	**POND**	**CAL**	
1	¿Existen procedimientos y/o políticas documentados del uso y manejo de la información?	**X**		**10**	5	
2	¿Están descritas las funciones y responsabilidades del personal que utiliza información de la entidad?	**X**		**10**	10	
3	¿Se lleva un control documentado cuando se solicita o se entrega una información?	**X**		**10**	10	
4	¿Usan mecanismos de bloqueo automático del computador en caso de estar inhabilitada por un periodo determinado?	**X**		**10**	5	Depende de cada empleado.
5	¿Las personas conocen, cuáles son sus funciones y de que son responsables en cuanto	**X**		**10**	10	

	al manejo de información de la carrera?					
6	¿Tienen clasificada la información, la que se puede acceder, y la que no se puede acceder?	**X**		**10**	10	
7	¿Se aplican controles de acceso, a la oficina y al archivo de la información (física, digital) de la carrera?	**X**		**10**	10	
8	¿Está normado que cada empleado bloque automáticamente el computador en caso de estar inhabilitada por un periodo determinado?		**X**	**10**	0	
9	¿Todos los sistemas y programas implementados para el cumplimiento de las actividades de la carrera trabajan con licencia?	**X**		**10**	10	Laboratorio y administrados
10	¿Los cambios de programas o software realizados alteran la actual operación de la carrera?		**X**	**10**	0	
11	¿Se lleva un control, de los sistemas y aplicaciones implementadas y de los que ya no se implementan en las estaciones de trabajo administrativas de la carrera?	**X**		**10**	5	

12	¿Se cuenta con copias de la información de la carrera, en lugar diferente al de la computadora de trabajo?	**X**		**10**	10	
13	¿Todas las estaciones de trabajo cuentan con software, sistema operativo y antivirus con licencia actualizadas?	**X**		**10**	10	
14	¿Poseen mecanismos de destrucción de información de la carrera?		**X**	**10**	0	
TOTALES		**11**	**3**			
Σ PONDERACIÓN TOTAL (PT)				**140**		
Σ CALIFICACIÓN TOTAL (CT)					**95**	
FIRMA Y SELLO DEL ENTREVISTADO				**FIRMA DEL ENTREVISTADOR**		

Fuente: Director de la Carrera Informática

Cuadro 4.6. Matriz de Riesgo - Confianza a la Protección de Activos Intangibles

MATRIZ DE RIESGO - CONFIANZA

Determinación del riesgo confianza:

CP: Calificación Porcentual

PT: Ponderación Total

CT: Calificación Total

$$\boldsymbol{CP} = \frac{CT * 100}{PT}$$

$$\boldsymbol{CP} = \frac{95 * 100}{140}$$

$$\boldsymbol{CP} = \mathbf{67,85}\%$$

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO
15 – 50	15 – 50	15 – 50
51 – 75	51 – 75	51 – 75
76 - 95	76 - 95	76 - 95

67,85

Nivel de confianza:	**MODERADO**	67,85%
Nivel de riesgo:	**MODERADO**	32,15%

El cuestionario de control interno aplicado al componente Protección de Activos Intangibles por 14 preguntas, obtuvo la contestación de 11 respuestas positivas y 3 respuestas negativas; obteniendo la ponderación total de 140 puntos y la calificación total de 95 puntos, lo que representa una calificación porcentual del 67,85%, determinando un nivel de riesgo moderado y a su vez el grado de confianza moderado.

Cuadro 4.7. Cuestionario de Control Interno aplicado a la Gestión de Mantenimiento

CARRERA INFORMÁTICA DE LA ESPAM MFL
CUESTIONARIOS DE CONTROL INTERNO

Componente: Gestión Mantenimiento de Hardware y Software

ÁREA AUDITADA: Carrera Informática	**FECHA DE APLICACIÓN:**
DIRIGIDO A: Ing. Armando Vidal	**FUNCIÓN:** Coordinador Mantenimiento

N°	PREGUNTAS	RESPUESTA		CUMPLIMIENTO		OBSERVACIONES
		SI	NO	POND	CAL	
1	¿Existe un control de acceso al área donde se da mantenimiento a los recursos tecnológicos?	**X**		**10**	5	No documentadas, accede solo personal autorizado.
2	¿Existen políticas de seguridad para el mantenimiento del software?		**X**	**10**	0	Procedimientos generales
3	¿Están descritas sus funciones y responsabilidades?	**X**		**10**	5	
4	¿Para el mantenimiento cuentan con software y aplicaciones con garantías vigentes?	**X**		**10**	10	Codificaciones para entidades educativas.

5	¿Existe un control de inventario de los recursos a los que se les da mantenimiento de software?		**X**	**10**	0	
6	¿Reciben los recursos tecnológicos mantenimiento de personas autorizadas?	**X**		**10**	10	
7	¿Se registran y documentan los fallos del software y de los recursos que se detectan en la carrera?		**X**	**10**	0	
8	¿Se tiene un historial de las peticiones de cambio en los sistemas?		**X**	**10**	0	
9	¿Realizan mantenimiento preventivo?	**X**		**10**	10	6 Meses
10	¿Realizan mantenimiento correctivo?	**X**		**10**	10	Se le notifica mediante llamadas telefónicas.
11	¿Los empleados y/o estudiantes pueden ejecutar programas de origen desconocidos en las estaciones de trabajo?		**X**	**10**	0	
12	¿Se lleva un control, de los sistemas y aplicaciones implementadas y de los que ya no se implementan en las estaciones de trabajo de los laboratorios de la carrera?		**X**	**10**	0	
13	¿Se lleva un control de las aplicaciones utilizadas y de las que ya no se utilizan?		**X**	**10**	0	

14	¿Se controla que las estaciones de trabajo en los laboratorios no estén configuradas con contraseña de inicio de sesión?		**X**	**10**	0	
15	¿Los equipos reciben mantenimiento dentro de las instalaciones?	**X**		**10**	10	Cuando es conveniente se los retira.
16	¿Los responsables de los recursos tecnológicos, le dan a conocer el daño de alguno de ellos?	**X**		**10**	5	Mediante notificaciones telefónicas
17	¿Tienen un lugar específico para guardar el material de mantenimiento de hardware?	**X**		**10**	10	
TOTALES		**9**	**8**			
Σ PONDERACIÓN TOTAL (PT)				**170**		
Σ CALIFICACIÓN TOTAL (CT)					**75**	
FIRMA Y SELLO DEL ENTREVISTADO				**FIRMA DEL ENTREVISTADOR**		

Fuente: Asistente de TIC

Cuadro 4.8. Matriz de Riesgo - Confianza de la Gestión de Mantenimiento

MATRIZ DE RIESGO - CONFIANZA

Determinación del riesgo confianza:

CP: Calificación Porcentual
PT: Ponderación Total
CT: Calificación Total

$$\boldsymbol{CP} = \frac{CT * 100}{PT}$$

$$\boldsymbol{CP} = \frac{75 * 100}{170}$$

$$\boldsymbol{CP} = \mathbf{41,17}\%$$

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO
15 – 50	BAJO	ALTO
51 – 75	MODERADO	MODERADO
76 - 95	ALTO	BAJO

44.11%

Nivel de confianza:	**BAJO**	44,11%
Nivel de riesgo:	**ALTO**	55,89%

El cuestionario de control interno aplicado al componente Gestión de Mantenimiento de 17 preguntas, se obtuvo la contestación de 9 respuestas positivas y 8 respuestas negativas; obteniendo la ponderación total de 170 puntos y la calificación total de 75 puntos, lo que representa una calificación porcentual del 44,11%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.

Cuadro 4.9. Cuestionario de Control Interno aplicado a la Gestión de Desarrollo de Software

CARRERA INFORMÁTICA DE LA ESPAM MFL
CUESTIONARIOS DE CONTROL INTERNO

Componente: Gestión de Desarrollo de Software

ÁREA AUDITADA: Carrera Informática	**FECHA DE APLICACIÓN:**
DIRIGIDO A: Ing. Harold Buenaventura	**FUNCIÓN:** Coordinador Unidad de Producción de Software

N°	PREGUNTAS	RESPUESTA		CUMPLIMIENTO		OBSERVACIONES
		SI	NO	POND	CAL	
1	¿Existen medidas, procedimientos definidos en una normativa de seguridad?	X		10	5	Involucran a los controles de la carrera.
2	¿Existe controles de seguridad en cuanto al acceso a la unidad?	X		10	5	
3	¿Existe procedimientos de seguridad mientras el coordinador no está el área, que garantice la protección del mismo?	X		10	5	Con sistema de vigilancia de la carrera.
4	¿Existen mecanismos de respaldo o copias de seguridad de información?	X		10	5	

5	¿Existen procedimientos para autorizar o conceder accesos a la base de datos del software que realizan?	**X**		**10**	10	Sólo personal, que desarrolla en la unidad.
6	¿Existe un período máximo de vida de las contraseñas?		**X**	**10**	0	
7	Los sistemas de autenticación de usuarios guardan, contraseñas encriptadas.	**X**		**10**	10	Estándar internacional
8	¿Existe procedimiento de asignación de contraseñas?		**X**	**10**	0	
9	¿Se registran los ingresos o salida de sus equipos tecnológicos?		**X**	**10**	0	
10	¿Mantienen actualizado, las aplicaciones para evitar, sustracción o daña de información, como antivirus, firewall, entre otros?	**X**		**10**	10	
TOTALES		**7**	**3**	**100**	**50**	
Σ PONDERACIÓN TOTAL (PT)						
Σ CALIFICACIÓN TOTAL (CT)						
FIRMA Y SELLO DEL ENTREVISTADO				**FIRMA DEL ENTREVISTADOR**		

Fuente: Coordinador de la Unidad de Producción de Software

Cuadro 4.10. Matriz de Riesgo - Confianza de la Gestión de Desarrollo de Software

MATRIZ DE RIESGO - CONFIANZA

Determinación del riesgo confianza:

CP: Calificación Porcentual
PT: Ponderación Total
CT: Calificación Total

$$\boldsymbol{CP} = \frac{CT * 100}{PT}$$

$$\boldsymbol{CP} = \frac{50 * 100}{100}$$

$$\boldsymbol{CP} = \mathbf{50}\%$$

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO
15 – 50	BAJO	ALTO
51 – 75	MODERADO	MODERADO
76 - 95	ALTO	BAJO

50%

Nivel de confianza:	**BAJO**	50%
Nivel de riesgo:	**ALTO**	50%

El cuestionario de control interno aplicado al componente Gestión de Mantenimiento de 10 preguntas, se obtuvo la contestación de 7 respuestas positivas y 3 respuestas negativas; obteniendo la ponderación total de 100 puntos y la calificación total de 50 puntos, lo que representa una calificación porcentual del 50%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.

Cuadro 4.11. Matriz general porcentual del nivel de Riesgo-Confianza

MATRIZ DE RIESGO-CONFIANZA									
Data Center		**Activos Tangibles**		**Activos Intangibles**		**Mantenimiento**		**Gestión Desarrollo de Software**	
Riesgo	Confianza	Riesgo	Confianza	Riesgo	Confianza	Riesgo	Confianza	Riesgo	Confianza
37,50%	62,50%	43,75%	56,25%	32,15%	67,85%	55,89%	44,11%	50%	50%

Fuente: Cuestionarios de Control Interno

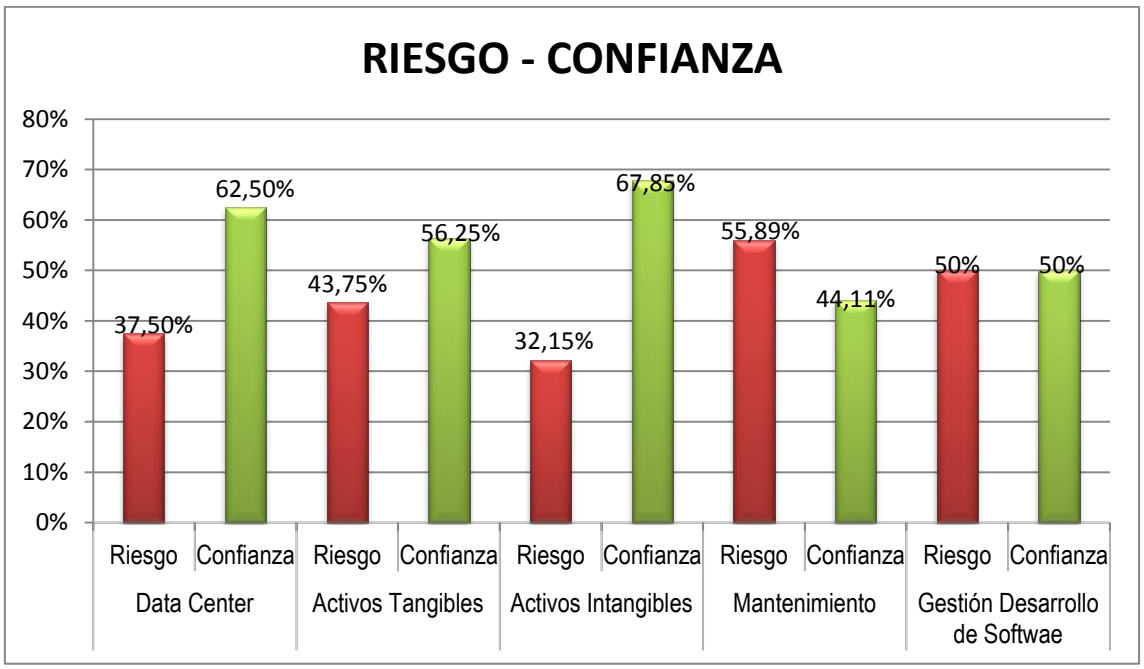


Gráfico 4.2. Nivel porcentual del Riesgo Confianza en la Carrera Informática

Como se observa en el gráfico 4.1. los datos presentados están basados en la calificación porcentual contemplada en la matriz de riesgo confianza del Manual de Auditoría para las entidades del sector público del Ecuador, emitido por la Contraloría General del Estado, por lo cual se definieron los siguientes resultados: en el Data Center, el nivel de confianza sobre las medidas de seguridad implantadas es de 62,50% frente a la proporcionalidad de riesgo de 37,50%, situación que se presenta por la aplicación de directrices generales de seguridad, debido a que no se han documentado políticas específicas de funcionamiento y protección de los recursos que posee esta área.

Por consiguiente, la protección de Activos Tangibles en la Carrera Informática tiene un nivel de confianza de 56,25% y la proporción de riesgo es de 43,75%; escenario que surge debido a que no se han establecido programas documentados de mantenimiento para los recursos tecnológicos, ni políticas de uso o medidas a seguir en caso de desastres; en la protección de Activos Intangibles el porcentaje de confianza es de 67,85%, ante un porcentaje proporcional de riesgo de 32,15%; las personas conocen, cuáles son sus funciones y de que son responsables en cuanto al manejo de información de la entidad, sin embargo, no existen procedimientos documentados que certifiquen dicha acción.

En la Gestión de Mantenimiento, el 44,11% corresponde a la confianza y el 55,89% es de riesgo; manteniéndose así, un nivel considerable de riesgo, debido a que no existen planes documentados que certifiquen el mantenimiento continuo y buen uso de los recursos que posee la entidad y por último la en la Gestión de Desarrollo de Software, el nivel de confianza es de 50%, y el riesgo es 50%.

Es así, que se evidencia que el sector con mayor nivel de confianza es la protección de los Activos Intangibles con una confianza de 67,85% y el componente con menor nivel de confianza es la Gestión de Mantenimiento con 44,11%.

Para saber la puntuación de concordancia entre las respuestas de las personas a las que se les aplicó el cuestionario, estos fueron analizados y se seleccionaron las preguntas en común de cada uno, para llegar a la conclusión y determinar el respectivo nivel de concordancia, para lo cual se desarrolló a través del Coeficiente de Concordancia de Kendall.

Antes de realizar la Prueba de Coeficiente de Concordancia de Kendall, se determinó la siguiente problemática, utilizando el Diagrama de Ishikawa:

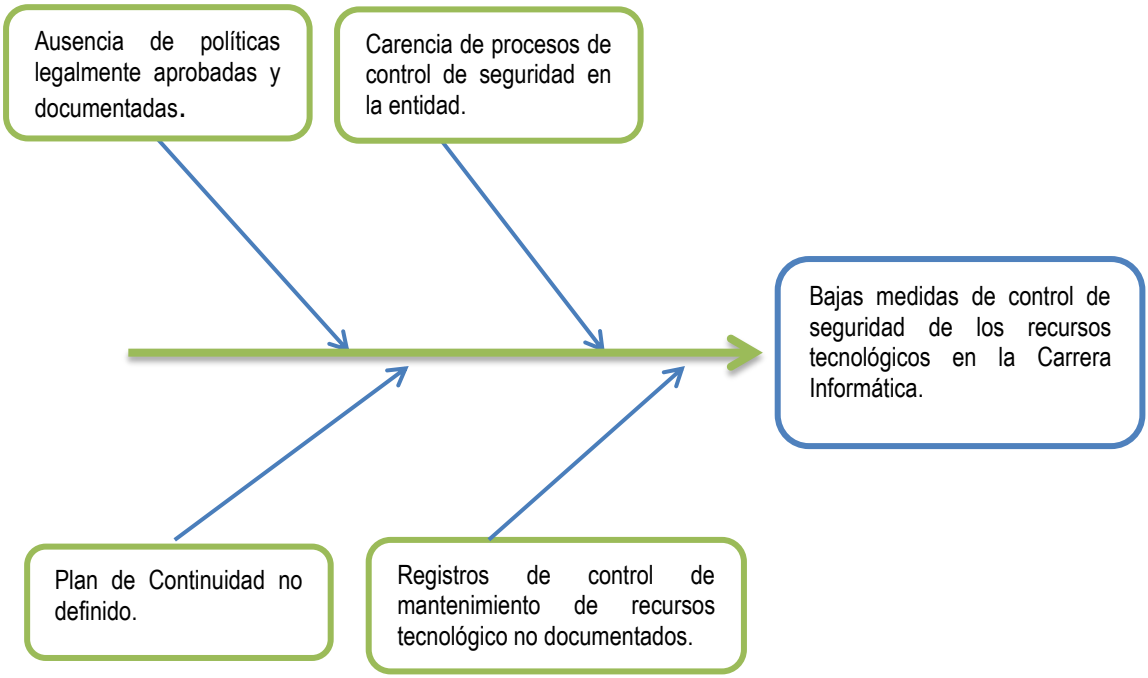


Figura 4.2. Diagrama de Ishikawa

Identificadas las causas que originan el problema, se realiza el siguiente cuadro, de aquellas preguntas similares, de las que se evaluaron las concordancias:

Cuadro 4.12. Concordancia de preguntas similares de los Cuestionarios Aplicados

Ítem K	Preguntas	Director de Carrera	Administración de Data center y Redes	Asistencia de TIC	Coordinador de UPS	∑aij	A	A^2
1	Existencia de Políticas de Seguridad documentadas.	4	4	3	4	15	5	25
2	Existencia de mecanismos de acceso físico al área.	2	1	2	2	7	-3	9
3	Existencia de registro de entrada y salida de recursos tecnológicos.	3	3	4	3	13	3	9
4	Existencia documentada de las funciones y responsabilidades en las áreas.	1	2	1	1	5	-5	25
						40		**68**

Fuente: Cuestionario de Control Interno

Ejecución de la fórmula del Coeficiente de Concordancia de Kendal

$$w = \frac{12\sum A^2}{n^2\, n(k^2 - 1)}$$

Cuadro 4.13. Remplazo de fórmulas para Coeficiente de Concordancia de Kendall

Determinar valor de A:	**Determinar el valor de T:**
$A = \sum aij - T$ $A = 15 - 10$ $A = 5$ Para la primera pregunta, y así hasta culminar.	$T = \frac{\sum aij}{K}$ $T = \frac{40}{4}$ $T = 10$

Remplazo de la fórmula
$w = \frac{12\sum A^2}{n^2\ 4(k^2 - 1)}$
$w = \frac{12(68)}{4^2\ 4(4^2 - 1)}$
$w = 0{,}85$

Con el dato obtenido, se concluye que el grado de coincidencia de las respuestas equivale a 0,85 determinando que existen concordancia en los resultados, por lo tanto, se afirma que la entidad auditada, cuenta con un bajo control documentado de políticas aprobadas, de registros de entrada y/o salida de los recursos tecnológicos, concuerdan además que sus funciones y responsabilidades son conocidas, y que se han tomado lineamientos generales de seguridad en las áreas.

Por consiguiente, para obtener la evidencia suficiente y competente que respalden la opinión de las autoras, se aplicaron los programas de auditoria por componentes **(Anexo 8)**, con la finalidad de comprobar si los controles establecidos por la entidad, operan tal como lo determinaron los responsables, el propósito fue aplicar pruebas de cumplimiento, recopilando así, información que sustente el trabajo realizado, cuyos resultados permitieron definir los hallazgos detectados en la Carrera Informática.

Cuadro 4.14. Hoja de Hallazgo Nº 01

CARRERA DE INFORMÁTICA DE LA ESPAM MFL

AUDITORIA DE SEGURIDAD FÍSICA Y LÓGICA DE LOS RECURSOS DE TECNOLOGÍA DE INFORMACIÓN DE LA CARRERA DE INFORMÁTICA DE LA ESPAM MFL

HOJA DE HALLAZGO Nº 01

PROCEDIMIENTO: Verificar la existencia de políticas o procedimientos legalmente aprobados y documentados, que permitan regular las actividades de seguridad, acceso y/o control interno.

CONDICIÓN: Se controlan los procedimientos de seguridad mediante lineamientos generales, sin embargo, como política no ha sido aprobada ni publicada legalmente en la Carrera Informática, lo que conlleva a no tener legalidad interna en el ejercicio de sus actividades.

CRITERIO: Según la de ***Norma de Control Interno 410*** titulada ***Tecnología de la Información,*** referente a la ***410-04 Políticas y procedimientos:***

La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria.

CAUSA: Las autoridades no han desarrollado las oportunas gestiones para dar cumplimiento a las normativas vigentes respecto a la seguridad informática en la carrera.

EFECTO: La ausencia de políticas de seguridad informática aprobadas legalmente, evidencia que el uso de los recursos de tecnología de información por parte de los usuarios, no está siendo gestionado, situación que incrementa las posibilidades de explotación de las vulnerabilidades.

CONCLUSIÓN

Mediante la evaluación de control interno, la observación realizada en la entidad, y de lo manifestado en el hallazgo, se concluye que la Carrera Informática practica en sus actividades lineamientos generales de seguridad, los cuales han sido adoptados para precautelar los equipos que poseen.

Sin embargo, dichos procesos no se encuentran documentados legalmente en una política de seguridad, que permita de forma clara explicar los fines de la misma, de manera que las personas involucradas en las actividades de la entidad sean administrativos, docentes, estudiantes de la carrera o de otra, que conozcan sobre las responsabilidades asumidas, con lo que respecta a la salvaguarda y prevención de los recursos de tecnología de información contra amenazas del medio.

Además la elaboración de una política de seguridad en la entidad auditada será de beneficioso para cumplir con futuras evaluaciones que les realicen, demostrando que cumplen con las leyes o normativas vigentes en el Ecuador, por lo que las autoridades deben asumir compromisos para aprobar, documentar y dar a conocer dichos procedimientos, con el propósito de que los involucrados en el proceso no se desvinculen.

RECOMENDACIONES

A LA DIRECCIÓN DE CARRERA

Decretar la realización, aprobación y publicación de una Política de Seguridad Informática en la entidad, que involucre temas de control de acceso a la red, ubicación de los recursos, acceso a las aulas, laboratorios, oficinas de docentes, y oficinas administrativas. Los mismos que sean procedimientos que apoyen la toma de decisiones ante incidentes de pérdida de un bien tangible o intangible, documentación de acuerdos de responsabilidades entre otras

direcciones o coordinaciones educativas que realicen sus actividades con los recursos tecnológicos y educativos de la entidad auditada.

Lo mencionado es considerado de carácter necesario para minimizar los peligros a los que están sujetos los activos y minimizar la interrupción de las actividades de la Carrera Informática.

Para definir la política de seguridad, se deberá tomar en cuenta la realización de la siguiente estructura:

- ✓ Una definición de seguridad de la información, objetivos generales y su alcance, así como la importancia de la seguridad como un mecanismo que permite que se comparta la información transparente.
- ✓ Una declaración de la intención de la máxima autoridad, que apoye las metas y los principios de seguridad de la información en línea con la estrategia y los objetivos de la Carrera.
- ✓ Una explicación breve de las políticas, principios, estándares y requisitos de cumplimiento de importancia particular para la organización, incluyendo:
  - ✓ Cumplimiento con los requerimientos legislativos, regulatorios y contractuales vigentes en el país.
  - ✓ Requerimientos de formación, capacitación concienciación en seguridad.

ASPECTOS A CONSIDERAR

- ✓ **Qué debe protegerse**: Todos los recursos tecnológicos y la información física o electrónica que exista en la Carrera Informática, definiendo la ubicación, acceso, registro de mantenimiento preventivo o correctivo, fuera o dentro de la entidad.
- ✓ **De qué debe protegerse:** De amenazas originadas por el ingreso no autorizado a la red, usando contraseñas ajenas, ingreso a las áreas como laboratorios de personas no autorizadas o que no hayan sido

registradas, robo, incendios, inundaciones, salida de información no autorizada.

- ✓ **Responsables de la protección:** Las personas que utilizan los recursos tecnológicos, directamente como el director, asistentes, secretaria, docentes, estudiantes de la Carrera Informática, entre otros. Indirectamente o terceras partes como, proveedores de servicios, docentes y estudiantes de otras coordinaciones, asumiendo todos roles y responsabilidades en la utilización del equipo en el uso exclusivo para propósitos legítimos de la entidad. Además los encargados de la asignación de autorización, y los custodios llaves.

Deben normarse las modificaciones que puede sufrir de acuerdo al cambio de la legislación ecuatoriana.

A LAS AUTORIDADES, EN CUANTO AL DATA CENTER

En base a los resultados de la evaluación de control interno, las visitas realizadas al departamento, y el hallazgo definido, se establece al Data Center, como eje trasversal en las actividades de la Carrera Informática y sobre todo de la ESPAM MFL, por ser el custodio de la información, además es el encargado de la administración de la red en la carrera, por ende necesita de carácter urgente la legalización de los lineamientos de seguridad adoptados por el administrador del mismo, ya que al poseer información importante sobre la entidad, debe estar sujeto a política documentada legalmente en cuanto a seguridad para la ejecución de sus operaciones, sean estos al cuarto de entrada, el área de distribución principal (MDA), el área de distribución horizontal (HDA), o el área de distribución de equipos (EDA). Con el fin de mejorar la seguridad aprovechando plenamente los beneficios del Centro de Datos consolidado y proporcionando una infraestructura administrable que cumpla con las normativas vigentes.

La política contendrá los principios y la estructura de la recomendación anterior a la de la Dirección, agregando:

ASPECTOS A CONSIDERAR

- ✓ **Qué debe protegerse**: Todos los recursos tecnológicos y la información física o electrónica que exista bajo la custodia del Data Center, definiendo la ubicación, acceso, registro de mantenimiento preventivo o correctivo, fuera o dentro de la entidad.
- ✓ **De qué debe protegerse:** De amenazas originadas por el ingreso no autorizado a la red la cuenta de un tercero, ya que:
  Establecer procedimientos en la asignación de cuentas; usuario y claves, estableciendo diferencia una de la otra.
  - ✓ Definir procedimientos sobre quiénes podrán autorizar el acceso al área.
  - ✓ Existir un procedimiento formal para el registro de cancelación de usuarios con el fin de gestionar el acceso a los sistemas o red.
  - ✓ Establecer los tipos de accesos tienen los diversos usuarios y emplear métodos apropiados de autenticación para controlar acceso de usuarios.
  - ✓ Todos los proceso que involucre, asignación, cambio, modificación o revocación de cuentas usuario es a través de procedimientos formales.
- ✓ **Responsables de la protección:** En primera instancia la persona que administre el Centro de Datos, además, las personas que tienen el acceso autorizado en el ingreso del mismo, y aquellas personas autorizadas a utilizar recursos tecnológicos como servidores, asumiendo todos roles y responsabilidades en la utilización de los equipos en el uso exclusivo para propósitos legítimos de la entidad.

Deben normarse que la política estará accesible a modificaciones, de acuerdo a cambios, agregación o disminución de procesos, o por cambios en la legislación ecuatoriana.

Cuadro 4.15. Hoja de hallazgo Nº 02

CARRERA DE INFORMÁTICA DE LA ESPAM MFL **AUDITORIA DE SEGURIDAD FÍSICA Y LÓGICA DE LOS RECURSOS DE TECNOLOGÍA DE INFORMACIÓN DE LA CARRERA DE INFORMÁTICA DE LA ESPAM MFL** **HOJA DE HALLAZGO Nº 02**
PROCEDIMIENTO: Comprobar la existencia de un Plan de Continuidad que proteja sus procedimientos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres.
CONDICIÓN: De acuerdo a la evaluación de control interno, se comprobó que la Carrera Informática no cuenta con políticas, procedimientos o planes legalmente constituidos, que le permitan asegurar la continuidad de sus operaciones ante cualquier vulnerabilidad, basado en el establecimiento de medidas preventivas.
CRITERIO: Según la ***Norma de Control Interno 410*** titulada ***Tecnología de la Información,*** referente a ***410-10 Seguridad de Tecnología de Información:*** La máxima autoridad, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos. Según la ***Norma de Control Interno 410*** titulada ***Tecnología de la Información,*** referente a ***410-11 Plan de Contingencias:*** Corresponde a la máxima autoridad 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.
CAUSA: Las autoridades no han garantizado que todos los procedimientos

de seguridad dentro de sus áreas de responsabilidad se llevan a cabo bajo el cumplimiento de Normas de Control.
EFECTO: Al no contar con la implementación de planes para la continuidad de las operaciones, la Carrera Informática, puede ser víctima de posibles incidentes, una caída de la luz eléctrica, una inundación, un incendio o un robo han de considerarse amenazas reales que deben ser tratadas de forma preventiva para evitar, en caso de que éstas sucedan, que las pérdidas no sean tan graves y que afecten a la viabilidad de sus actividades.

CONCLUSIÓN

La Carrera Informática no cuenta con un Plan de Continuidad, que le permita seguir ante las posibles amenazas a las que está expuesta, lo que puede conllevar desde una pérdida importante de las prestaciones de servicios hasta un desastre natural, sin embargo, ante esta situación es imprescindible estar preparados con procedimientos, políticas y planes que mitiguen los riesgos. Por lo tanto, resulta necesario implementar un Plan de Continuidad que permita tener una respuesta efectiva a las interrupciones de las operaciones y cumplir con las disposiciones legales.

RECOMENDACIONES

A LA DIRECCIÓN DE CARRERA

Declarar la elaboración, aprobación e implementación de un Plan de Continuidad considerado necesario para minimizar las consecuencias de la interrupción del servicio. Para lo cual, se deben considerar los siguientes aspectos:

No sólo las catástrofes ambientales, tales como incendios o inundaciones, pueden causar daños adversos a la entidad, otros tipos de incidentes, como los

que se detallan a continuación, pueden tener impactos adversos en la Carrera Informática.

- ✓ Incidentes de seguridad en los sistemas, como delitos cibernéticos, pérdida de información, robo de información sensible o su distribución accidental, fallos en los sistemas, errores de operación en los sistemas, entre otros.
- ✓ Daños en las infraestructuras o en los servicios, fallos en el suministro eléctrico, fallos en el suministro de agua, fallos en las comunicaciones, entre otros.
- ✓ Fallos en los equipos o en los sistemas, incluyendo fallos en las fuentes de alimentación.
- ✓ Fallos en los servicios en los servicios de comunicación.

El plan establecerá, organizará y documentará los riesgos, responsabilidades, políticas, procedimientos y acuerdos, así mismo, proporcionará un enfoque organizado y consolidado para dirigir actividades de respuesta y recuperación ante cualquier incidente o interrupción de operaciones imprevista, evitando confusión y reduciendo la situación de tensión. El plan debe estar documentado, basado en los siguientes lineamientos:

1. Creación de una política de continuidad del negocio:

Elaborar una política que defina la magnitud y el alcance de la continuidad de las operaciones dentro de la entidad. Debe estar documentada y orientada a sustentar un conjunto de principios basados en las necesidades de la Carrera Informática y el entendimiento de los riesgos asociados. A su vez debe ser proactiva y abarcar controles preventivos, de detección y correctivos. El mensaje que se debe transmitir a la entidad es que se tienen que usar todos los controles posibles para detectar y evitar interrupciones y que, aunque ocurran, se deben tener los controles necesarios para mitigar las consecuencias.

2. Análisis de Impacto

Obtener conocimiento de los procesos que se consideran críticos para el funcionamiento de la Carrera Informática. Una vez identificados, se analizarán cuáles son los riesgos asociados a dichos procesos para identificar, cuáles son las causas potenciales que pueden llegar a interrumpir las operaciones.

Se deben identificar los diversos eventos que podrían tener un impacto sobre la continuidad de las operaciones. Resultado que se obtiene a partir de la evaluación de riesgos.

3. Estrategia de Recuperación

Identificar la mejor manera de recuperar un sistema en caso de interrupción. Se deben valorar las diferentes alternativas y estrategias de respaldo en función de los resultados obtenidos en el análisis del impacto, para seleccionar la más adecuada a las necesidades de la entidad.

4. Desarrollo del Plan de Continuidad

Los diferentes factores que se deben considerar cuando se desarrolla el plan son los siguientes:

- ✓ Capacidad para actuar antes de que ocurran desastres, que cubra el manejo de la respuesta a incidentes con el fin de resolver correctamente todos los incidentes relevantes que afecten los procesos de negocios.
- ✓ Procedimientos de evacuación.
- ✓ Procedimientos para la declaración de un desastre.
- ✓ Circunstancias bajo las cuales se debe declarar un desastre, todas las interrupciones no representan desastres, por un mínimo incidente si no se manejan a tiempo o de una manera adecuada, podrían conducir a un desastre.
- ✓ La identificación clara de las responsabilidades en el plan.

- ✓ La explicación paso a paso del proceso de recuperación.
- ✓ La identificación clara de los diferentes recursos que se requieren para la operación de recuperación y continuidad de la entidad.

5. Pruebas y Mantenimiento del Plan de Continuidad

Verificar el funcionamiento del Plan de Continuidad, mediante la estrategia de pruebas, determinando que realmente funciona y es efectivo. Además, se definirán los procedimientos de mantenimiento del Plan.

Debe normase que el Plan de Continuidad estará accesible a modificaciones de acuerdo a cambios, agregación o disminución de procesos, o cambios en la legislación ecuatoriana.

Cuadro 4.16. Hoja de Hallazgo Nº 03

CARRERA DE INFORMÁTICA DE LA ESPAM MFL **AUDITORIA DE SEGURIDAD FÍSICA Y LÓGICA DE LOS RECURSOS DE TECNOLOGÍA DE INFORMACIÓN DE LA CARRERA DE INFORMÁTICA DE LA ESPAM MFL** **HOJA DE HALLAZGO Nº 03**
PROCEDIMIENTO: Verificar si existen registros de mantenimiento a los recursos tecnológicos de la Carrera Informática.
CONDICIÓN: Conforme a la evaluación de control interno, se detectó que la Carrera Informática no cuenta registros documentados del mantenimiento de recursos tecnológicos.
CRITERIO: Según la ***Norma de Control Interno 410*** titulada ***Tecnología de la Información,*** referente a ***410-10 Mantenimiento y control de la infraestructura tecnológica*** La unidad de tecnología de información de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades.
CAUSA: El departamento de Soporte Técnico brinda mantenimiento a los recursos tecnológicos de la ESPAM MFL en general, por ende no existen medidas establecidas que determinen las condiciones (Lugar, calendario, horario) en que debe llevarse el mantenimiento a los equipos y sistemas de la Carrera Informática, lo que genera inconvenientes a la hora de mejorar el desempeño y buen uso de los recursos tecnológicos.
EFECTO: En consecuencia el no contar con medidas establecidas para el mantenimiento de los recursos tecnológicos, estos se ven afectados, provocando fallos en su rendimiento.

CONCLUSIÓN

La Carrera Informática no cuenta con programas que garanticen el apropiado mantenimiento de sus recursos tecnológicos, razón por la cual estos son propensos a sufrir daños. Sin embargo, para el cumplimiento de los objetivos de la Carrera Informática, se requiere de una actividad programada de inspecciones, tanto de funcionamiento como de seguridad, ajustes, reparaciones, análisis, desempeño, que deben llevarse a cabo en forma periódica en base a un plan establecido. El propósito es prever averías o corregirlas para mantener las instalaciones, equipos y sistemas en niveles óptimos de operación.

RECOMENDACIONES

A LA DIRECCIÓN DE CARRERA

- ✓ Realizar una planificación vinculada con el Departamento de Mantenimiento y Soporte Técnico de la ESPAM MFL, con la finalidad de mantener la infraestructura y equipos de la Carrera Informática en condiciones óptimas para lograr la conformidad con los requisitos del servicio educativo, considerando los siguientes aspectos.

- ✓ Establecer políticas orientadas a brindar mantenimiento a los recursos tecnológicos.

- ✓ Elaborar inventarios actualizados de los recursos tecnológicos que posee la Carrera Informática, con la finalidad de facilitar las tareas de mantenimiento.

- ✓ Determinar la necesidad de mantenimiento mediante la elaboración de una solicitud.

- ✓ El Dpto. de Mantenimiento y Soporte Técnico, debe realizar listas de verificaciones con el fin de verificar las instalaciones, evaluando espacios y equipos que necesitan de revisión.

- ✓ Elaborar un Programa de Mantenimiento con base a las lista de verificaciones, y atendiendo a las solicitudes recibidas.

- ✓ Elaborar y presentar los informes periódicos de las actividades realizadas, con el propósito de obtener un registro de los recursos a los cuales se les proporciono mantenimiento y soporte técnico.

Concluyendo con la investigación, se presenta el Informe Final de Auditoría **(Anexo 6)** en el que se determina de manera resumida, centrados en los hallazgos identificando las conclusiones y recomendaciones propuestas para la entidad auditada.

Ejecutado el proceso de la auditoría, se determinó que la información es el activo más importante para las organizaciones, por este motivo la información adquiere gran importancia, las entidades deben velar por tener niveles de seguridad confiables, convirtiéndose en una inversión adicional para todas las entidades, los especialistas concuerdan en que no es posible conseguir un 100% de seguridad, es necesario establecer un balance entre el nivel de inversión y el nivel de seguridad que se desea obtener.

Recurrir a firmas consultoras para ejecutar auditorías de seguridad informática en las organizaciones es una táctica. El consultor debe indicarle a la entidad cuáles son sus puntos débiles, para luego pasar a desarrollar una estrategia y así, generar mejor efectividad en los procesos instaurados

El auditor informático debe velar por la correcta utilización de recursos que la entidad pone en juego para disponer de un eficiente y eficaz sistema de información. En las entidades públicas su importancia radica en proporcionar

una seguridad razonable de que se protegen los recursos públicos adecuadamente y se alcancen los objetivos institucionales

El costo de una auditoría varía en función del volumen del trabajo que tenga que realizar el auditor y lógicamente, de sus habilidades y experiencia. Realizar auditorías informáticas de forma periódica es importante para toda organización que aprecie el gasto que puede ocasionar el uso indebido de los recursos; pero aún lo es más importante para aquellas que cuidan el riesgo legal que puede motivar una conducta inapropiada de sus empleados en el uso de los sistemas informáticos, teniendo en cuenta que las entidades del sector público están bajo control y supervisión de la Contraloría General del Estado.

En relación a lo mencionado anteriormente, las autoras realizan sugerencias positivas, prácticas constructivas, a fin de dar soluciones a las deficiencias encontradas en el transcurso de la auditoría. Estas constituyen la parte más importante del informe, y deben ser de aplicabilidad inmediata siempre analizando el beneficio para la Carrera Informática.

4.2. DISCUSIÓN

Para el desarrollo de la Auditoría de Seguridad Física y Lógica a los Recursos de Tecnología de Información en la Carrera Informática de la ESPAM MFL, se aplicaron las fases de auditoria determinadas en las Normas Internacionales de Auditoría, emitidas por el Consejo de Normas Internacionales y Aseguramiento IAASB órgano encargado de la emisión de las mismas, con el objetivo de promover la calidad y la uniformidad de la práctica a nivel mundial, además se realizó la evaluación de control interno, determinada en las Normas de Control Interno, emitidas por la Contraloría General del Estado, ente regulador de las entidades del sector público; con la finalidad de determinar el nivel de riesgo y el grado de confianza, de los componentes a ser examinados, obteniendo así, información en la cual se fundamentan los hallazgos.

En comparación de otros trabajos, con el fin de encontrar la realización de un auditoría de seguridad, cuyas características fueran lo más similar a la aplicada en la Carrera Informática, posterior a revisar diversas tesis y artículos ejecutados, se analizaron las tesis de maestría, Análisis de la auditoria en seguridad informática del departamento de tecnologías de la Universidad Estatal de Milagro, del autor, Javier Ricardo Bermeo Paucar (Bermeo, 2012), en la cual el autor realizó su investigación y análisis mediante la aplicación detallada de cada actividad de auditoría como fase de la misma, obteniendo de esta manera nueve fases, su investigación se basó en las Normas de Control Interno referente Tecnologías de Información, emitidas por la Contraloría General del Estado, y base legal vigente en el país

Así mismo, se analizó la tesis previa al diplomado en auditoria informática, titulada Auditoria a Centros de Computo en base a la metodología de control interno, de las autoras María Fernanda Cortes Saavedra y Jessica Carolina Machuca De La Torre (Cortes y Machuca, 2011), para lo cual platean como metodología el uso de las Normas Internacionales de Auditoria y la aplicación de una evaluación de control interno que le permita calificar la eficacia de los controles relacionados con la confiabilidad de la información.

Las autoras del presente trabajo concuerdan con los demás autores en la aplicación de la Normativa legal vigente en el país, que permite evaluar el control interno en el uso de los recursos tecnológicos de las entidades auditadas, cuya metodología sirve de referente para posteriores evaluaciones proporcionando seguridad en la ejecución de los procesos de la entidad. Sin embargo para mayor confiabilidad de datos se realizó un método estadístico no paramétrico, el Coeficiente de Concordancia de Kendall, para determinar el nivel de concordancia entre las respuestas que dieron las personas a las que se les aplicó el cuestionario.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Una vez finalizada la auditoría de seguridad física y lógica a los recursos de tecnología de información de la Carrera Informática, las autoras concluyen lo siguiente:

- La metodología aplicada se adaptó al desarrollo de la auditoría, y aportó a través de cada una de sus fases, a las actividades y procedimientos a seguir, con la finalidad de alcanzar el objetivo propuesto.

- El estudio y diagnóstico de la situación actual, permitió conocer las necesidades existentes para las distintas áreas de la carrera, en la que se registra inexistencia de manuales, políticas y procesos a cumplir.

- La ausencia de una normativa de seguridad para una adecuada evaluación y control de los recursos de TI, trae como consecuencias que estos operen en ambientes poco seguros y confiables.

- La aplicación de técnicas de auditoría, resultaron de gran utilidad, permitiendo obtener información acerca de las operaciones, que se desarrollan en la carrera, pudiendo así, describir en forma detallada los hallazgos encontrados durante la ejecución de la misma.

5.2. RECOMENDACIONES

Concluida la auditoría de seguridad física y lógica a los recursos de tecnología de información de la Carrera Informática, las autoras recomiendan lo siguiente:

- Previo a la planificación de una auditoría, se deben conocer las posibles metodologías a aplicarse, acorde a los lineamientos a auditar en las áreas de cada entidad.

- Es conveniente que las entidades públicas realicen sus políticas y planificaciones para que la seguridad física y lógica de los recursos tecnológicos surja como un instrumento para concienciar a las personas que conforman la carrera sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la entidad desarrollarse.

- Implementar normas o estándares de seguridad para la protección de los recursos tecnológicos en la entidad, para minimizar los posibles riesgos a la infraestructura o a la información.

- En el desarrollo de una auditoría, se deben aplicar técnicas que se acoplen a la situación actual de la entidad auditada, para obtener la información suficiente y competente, que permita sustentar objetivamente los hallazgos evidenciados.

BIBLIOGRAFÍA

Acuerdo Nº 039 CG. 2009. Normas de Control Interno para las entidades, organismos del sector público y personas jurídica de derecho privado que dispongan de recursos públicos. San Francisco de Quito, EC. 16 de nov.

Álvarez, R. 1995. Coeficiente de concordancia de Kendall. Díaz de Santos, S.A., Madrid, ES. p 346.

Armas, R. 2006. Auditoría en Sistemas Informáticos y Control de la Información. 1 ed. Ecuador.

Arroyo, M. 2013, La importancia de la auditoría de seguridad informática. (En línea). Fortmato HTML. Consultado 20 de ene de 2014. Disponible en http://www.proxyconsulting.es/?p=85

Baldeón, M. 2012. Plan maestro de seguridad informática con lineamiento de la norma ISO 27002. p 2. México.

Barchini, G; Sosa, M; Herrera, S. s.f. La informática como disciplina científica. Universidad Nacional de Santiago del Estero. AR.

Bernal, R. 2006. Auditoria de los sistemas de información. Universidad politécnica de Valencia. p. 64.

Carrasco, A. 2013. Conceptos de seguridad informática y su reflejo en la cámara de cuentas de Andalucía. Revista Auditoría Pública. Sevilla, ES. Nº 61. p 11-117.

Castilla, J. 2007. Manual de Outsorurcing Informático. 2 ed. Ediciones Días de Santos S.A. Madrid España. p. 86.

Castro, E. 2009. Tendencias de la auditoria informática. Cali, CO. Revista Ingenlum Ciencia & Tecnología. Vol. 4, Nº 8. P, 69- 98.

Cepeda, G. 2008. Auditoría y Control Interno. 2 ed. Editora Emma Ariza Herrera. Colombia.

CGE (Contraloría General del Estado), 2003. Manual General de Auditoría Gubernamental de las Entidades y Organismo del Sector Público y para las Firmas privadas de auditorías contratadas. Acuerdo 012-CG-2003, RO 107 19 de Jun de 2003

Cortes, M; Machuca, J. 2011. Auditoría de Centros de Cómputo. Escuela Superior Politécnica del Litoral. p. 58.

Davara, M. 2004. An introduction to computer security. The NIST. National Institute of Standards and Technology. Special publication 800 -12.

Day, K. 2003. Inside the security mind. Revista digital zing@. Publicación nº 34, Vol 4.

Delgado A. 2009. Sistema Informático de Apoyo a la Evaluación del Control Interno. Revista de Arquitectura e Ingeniería, Vol. 3, Nº 1. p 4.

Donaire, P. 2011. Medidas Técnicas. Revista Narure. Vol 5.

Dussan, C. 2008, Políticas de Seguridad Informática. Entramado, CO. Vol. 2. Nº. 1. p. 86-92.

Fernández, A. 2005. Amenazas informáticas. Puebla, MX. Artículo de divulgación científica Nº. 2000. p. 6.

Fernández, J. 2000. Actualidad informática. Madrid, ES. Revista Arazandi Nº 34. p. 7 – 9.

Fitzgerald, J. 2003. Security in Computer System. Madrid, ES. Revista Deloitte. Vol. 45. p. 50 – 52.

Galdámez, P. 2003. Seguridad Informática. Actualidad TIC. Instituto Tecnológico de Informática ITI. Universidad Politécnica de Valencia. Valencia, ES. Boletín trimestral Nº 1. p. 4.

Gómez, R. 2010, Generalidades de la auditoría Informática. (En línea) Formato HTML. Consultado 27 de ene de 2014. Disponible en http://goo.gl/CcQUhs

González, M. 2009. Auditorias de Información. ACIMED. Habana, CU. Vol. 19. Nº 4. p 3.

Govindan, M. 2007. Control Interno, Auditoría y Seguridad Informática. Tomo II – IV. España.

Granados, A. 2012. Auditoría del desarrollo de sistemas de información en el Gobierno regional Cajamarca. Tesis. Ing. Sistemas Computacionales. Universidad privada del Norte. Cajamarca-Cajamarca, PE. p 8.

Hernández, A. 2010. Auditoria Informática y Gestión de Tecnologías de Información y Comunicación. Compendiun, VE. Vol. 13. Nº. 25. p 4.

Hervada, F. 2007). Gobierno de las Tecnologías y Sistemas de Información. 3ed. Madrid, ES. RA-MA. p. 75.

IAASB (Consejo de Normas Internacionales de Auditoría y Aseguramiento). 2009. Normas Internacionales de Auditoría. Vigentes en el país desde 2009.

Innovation Group S.L. s.f. Control Interno. (En línea). ES. Consultado, 28 de nov. 2013. Formato HTML. Disponible en http://auditoriasistemas.com/auditoria-informatica/control-interno/

ISACA (Asociación de Auditoría y Control de Sistemas de Información), 2006. Automating System Security Audits. Information Systems Control Journal. Vol. 1. p. 45 – 46.

Jamare, J. 2010. La seguridad informática. Metodología. Ediciones Arcadia. Madrid, ES.

James, M. 2009. Medidas de Seguridad. Pereira, CO. Revista Tecnológica de la Universidad Tecnológica de Pereira. Año XV, Nº x. p. 12.

Jiménez, J. 2008. La seguridad informática y el usuario final. Revista UNAM. MX. Vol.9, N 4. p. 4

Kuna, H; García, R; Villatoro, F. 2012. Procedimientos de la explotación de información para la identificación de datos faltantes, con ruido e inconsistentes. AR. p 2.

Lamere, J. 2009. La Seguridad Informática. Metodologías. 2 ed. Arcadia, ES. p. 56.

Lara A. 2010. Aplicación de la teoría de los procesos de la auditoría informática. Sangolquí, EC. Revista Digital ESPE. Vol. 25.

Ley Nº 24. 2004. Ley Orgánica de Transparencia y Acceso a la Información Pública. Publicado en el Registro Oficial Suplemento 337. Quito, EC. 18 de mayo.

Ley Nº 73. 2002. Ley Orgánica de la Contraloría General del Estado, publicada en el Registro Oficial número 595. San Francisco de Quito, EC. 12 de junio.

Madarriaga, M. 2006. Manual Práctico de auditoría. Barcelona, ES. p 40 – 55.

Maldonado, E. 2008. Auditoría de Informática. 6 ed. Editorial Producción Digitales Abya – Yala. Quito.

Martínez, A. 2012. Auditoria con Informática. Revista de arquitectura e Ingeniería. Vol. 6. Nº 2. p 3. Cuba.

Martínez, A; Blanco, B; Loy M. 2012. Auditoría con Informática a Sistemas Contables.Revista de Arquitectura e Ingeniería, Vol. 6, Nº 2. p 1-14.

Martínez L; 2009. El control interno: Un medio eficaz para la toma de decisiones en el control de la gestión. Bibliociencias. CU. p 19.

Martínez, Y. 2012. Auditoria en Informática. CU. Revista de Ingeniería. Vol. 6. Nº 2, p. 14.

Morant, A. y Sancho Z. 2009. Seguridad y protección de la información. Estudios Ramón Areces SA. Madrid, ES. p. 25.

Morlanes, G. 2012. Seguridad Informática, Matanzas, CU. Revista de Arquitectura e Ingeniería, vol. 6, Nº 2. p. 1-14.

Muñoz, C. 2002. Auditoría de Sistemas Computacionales. 6 ed. Editorial Pearson Educación. México. p 66 - 130.

Navarro, E. 2005. Manual de dictámenes y peritajes informáticos. 2ed. Madrid, ES. Ediciones Díaz de Santos. p. 54.

Pérez, H. 2007. Estadísticas para las ciencias sociales, del comportamiento y de la salud, 3ed, MX. Cengaee Learning Editores S.A. P. 545-547

Piattini, M; Del Peso, E.; Del Peso, M. 2008. Auditoria de Tecnologías y Sistemas de Información. 4ed. Madrid, ES. RA-MAl. Vol. 1378. p 38.

Pinket, F. 2006. Automating System Security Audits. Information Systems Control Journal. ISACA. Vol 1. p 45 – 46.

Pons, F. 2007. Auditoría Informática, una aproximación a la mejora del control interno. Revista, Auditoría Pública, Sevilla, ES. Nº 41. p 97-100.

Ramírez, A. 2012. Riesgo tecnológico y su impacto para las organizaciones. Seguridad Cultura de prevención para las TIs. MX. Nº 14. p 09.

Ramírez, G. y Álvarez, E. 2008. Auditoría a la gestión de las tecnologías y sistemas de información. PE. Vol. 6. Nº. 1. p. 99.

Ramos, F. s.f. Guide to minimizing computer theft. Information tecnology security Branch. Publication 450 -01. p. 37

Ramos, M. 2002. La seguridad de los datos. Madrid, ES. Revista Ingenlum. Vol. 28. P. 6.

Rodríguez, A. 2010. La seguridad informática una necesidad en la docencia universitaria. CU. Revista IPLAC. Nº 1. p.

Romero, S. 2012. Técnicas para auditorías informáticas. Bogotá D.C, CO. Journal of Technology. Vol. 11. No. 1. p. 9 - 23.

Romo, D; Valarezo, J. 2012. Análisis e implementación de la norma ISO 27002 para el departamento de sistemas de la Universidad Politécnica Salesiana sede Guayaquil. Tesis, Politécnica Salesiana de Guayaquil. Guayaquil, EC. p 18.

Ruiz, T. 2012. Utilización del Método de los expertos (Delfos) para la validación de una estrategia pedagógica. Órbita Científica. Vol, 18. Nº 69. p. 1-12.

Sánchez H. 2011. Estrategias de control interno para la gerencia pública. Revista UIS humanidades Vol. 39, Nº 2. p 26.

SEDISI (Asociación Española de Empresas Tecnológicas de la Información, ES). 2007. Guía de la seguridad informática. Publicación Nº 003 – 50. p. 12.

Troyano, R. 2006. Auditoria informática. Revista Contabilidad. Vol. 45. p. 4.

Valle, R; Ros, F; Barberá, J; Gamella, M. 1986.Tecnologías de la información: electrónica, informática y telecomunicaciones, editado en Notas del curso Fundamentos y función de la ingeniería, ETSI Telecomunicación, Madrid (tomado del libro Los países industrializados ante las nuevas tecnologías, FUNDESCO).

Viloria, N. La importancia del concepto de independencia para la auditoría Actualidad Contable Faces, Vol. 12, Nº 18. p. 115-124.

Villardefrancos, A y Rivera, Z. 2008. La auditoría como proceso de control. Ciencias de la Información. Vol. 13. Nº 2-3. p. 53-59.

Whitten, J. 2008. Análisis y Diseño de Sistemas de Información. 2 ed. Editorial McGraw Hill Interamericana. Argentina. Buenos Aires.

ANEXOS

ANEXO 1

CARTA DE AUTORIZACIÓN

ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

República del Ecuador

RECTORADO

Oficio Nº: ESPAM MFL – R – 2013 – 339 – OF
Calceta, 19 de septiembre de 2013

Ingeniero
Luis Cedeño Valarezo
DIRECTOR DE LA CARRERA INFORMÁTICA DE LA ESPAM MFL
Ciudad.-

De mi consideración:

De conformidad a lo dispuesto en el oficio SN de fecha 18 de septiembre de 2013, sobre la realización de una tesis de grado en la Carrera Informática, autorizo a usted para que se realice la ejecución de dicha tesis titulada **"AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA A LOS RECURSOS DE TECNOLOGÍA DE INFORMACIÓN EN LA CARRERA INFORMÁTICA DE LA ESPAM MFL"**, a las áreas de Dirección de Carrera, Secretaría, Desarrollo de Software, Mantenimiento y Soporte Técnico, Centro de Datos, Redes, Aulas, Laboratorios y otras dependencias involucradas.

Los objetivos de la auditoría son:

- Comprobar la existencia de elementos que brinden salvaguarda a la infraestructura física de la carrera.
- Identificar controles de tecnologías de información.
- Verificar el nivel de cumplimiento de las políticas, planes y procedimientos que emplea la carrera en cuanto al uso de los recursos tecnológicos.
- Evaluar vulnerabilidades de una interrupción del servicio.
- Elaborar el informe de auditoría en la seguridad física y lógica considerando todos los hallazgos encontrados.

El tiempo estimado para la ejecución de la auditoría es de 90 días laborables en la entidad, a partir del lunes 30 de septiembre del presente año hasta el 28 de febrero del 2014; y el equipo de auditoría estará integrado por las señoritas Verónica Alexandra Espinoza Castillo y Amarilis Carolina Loor Párraga, por lo que dispongo que se preste la colaboración necesaria para la ejecución del trabajo indicado.

Atentamente,

Leonardo Félix López
RECTOR

LFL/dzm

ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ "MANUEL FÉLIX LÓPEZ" ESPAM "MFL" RECIBIDO Fecha: 19-09-2013 Hora: 16H00 CARRERA INFORMÁTICA

1/1

ANEXO 2

PLAN DE AUDITORÍA

CARRERA DE INFORMÁTICA DE LA ESPAM MFL PLAN DE AUDITORÍA	
DEPENDENCIA:	Carrera de Informática de la ESPAM MFL
OBJETIVOS:	**a.** Comprobar el control interno de la entidad, verificando sus puntos fuertes y débiles. **b.** Verificar el nivel de cumplimiento de las políticas, normas y procedimientos en cuanto al uso de los recursos tecnológicos. **c.** Comprobar el grado de seguridad del ambiente informático, cumpliendo con los objetivos de control y los objetivos institucionales. **d.** Presentación de un informe para dar a conocer los hallazgos encontrados, con sus respectivas conclusiones y recomendaciones.
ALCANCE:	El proceso de Auditoría de Seguridad Física y Lógica se realizará en la Carrera Informática, en las áreas de la Unidad de Producción de Software, Centro de datos, Dirección de Carrera, Inventario, Mantenimiento, Secretaría, Redes, la misma que ha proporcionado total apertura en las diferentes áreas. La evaluación comprende: **a. Evaluación de la dirección de informática en lo que corresponde a:** • Los procesos que se llevan a cabo. • Estructura Orgánica y Funcional. • Normas, políticas y procedimientos. • Planes de trabajo. • Controles. • Estándares. • Estudio de viabilidad • Convenios que se tiene con otras instalaciones. • Fechas de instalación y planes de instalación de

ALCANCE:	sistemas y equipos. • Contratos vigentes de compra y servicio de mantenimiento. • Contrato de Seguros. **b. Evaluación de los sistemas** • Evaluación de los diferentes sistemas de operación (flujo de información, procedimientos, documentación, redundancia, organización de archivos, estándares de programación, controles, utilización de los sistemas). • Seguridad física y lógica de los sistemas, su confidencialidad y respaldos • Descripción general de los sistemas instalados y de los que estén por instalarse, que contengan volúmenes de información. • Manual de formas. • Manual de procedimientos. • Descripción genérica. • Diagramas de funcionamiento. • Fechas de instalación de los sistemas. • Proyectos de nuevos sistemas. • Sistemas dados de bajos. **c. Evaluación de los equipos** • Número de equipos, localización y las características (equipos instalados y por instalarse). • Configuración de equipos y capacidades actuales y máximas. • Planes de expansión. • Ubicación general de los equipos. • Políticas de operación. • Políticas de uso de los equipos. • Proyectos de nuevos equipos.

DOCUMENTOS A SOLICITAR:	**a) Información General:** ▪ Estructura del ambiente de procesamiento de los sistemas de computación, sistemas de seguridad y redes. ▪ Estructura de presupuesto, activos con que cuenta, ciclos de operación. ▪ Controles gerenciales y manual de funciones de usuarios (segregación de funciones). ▪ Estructura del centro de cómputos, expedientes de personal del mismo, y a nivel de usuarios. ▪ Manuales, políticas y procedimientos de operaciones. ▪ Manuales de desarrollo, adquisición y mantenimiento de los sistemas de información (Soporte Técnico). ▪ Documentación sobre los sistemas de seguridad lógica y física y de los procesos de sistemas de información. **b) Seguridad** ▪ Solicitar las políticas de respaldo interno. ▪ Seguridad en los ambientes de los sistemas de control en la base de datos. ▪ Inventario y ubicación de los extintores e extinguidores, detectores de humos, adecuación de instalaciones. ▪ Accesos lógicos y físicos en el centro de cómputo, así como en su ambiente computacional y redes. **c) Integridad, confidencialidad y disponibilidad de los sistemas de información.** ▪ La utilización y almacenamiento de los códigos fuentes, licencia de los sistemas utilizados. ▪ Obtener los planes de contingencia y pruebas de controles de usuarios. **d) Desarrollo, adquisición y mantenimiento de los sistemas de información.** ▪ Manuales y guías sobre los soportes de las redes, software y hardware y sistemas de aplicaciones. ▪ Principales operaciones de los sistemas de

	información.
DOCUMENTO DE REFERENCIA	Se tomará como documento de referencia: Norma ISO/IEC 27002, Normas de Control Interno 410.

ANEXO 3

PROGRAMA GENERAL PARA LA PLANIFICACIÓN PRELIMINAR

CARRERA INFORMÁTICA

AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA A LOS RECURSOS DE TECNOLOGÍA DE INFORMACIÓN EN LA CARRERA INFORMÁTICA DE LA ESPAM MFL

PROGRAMA GENERAL PARA LA PLANIFICACIÓN PRELIMINAR

N°	OBJETIVOS:	REFERENCIA	HECHO POR
	Objetivos • Comprender la situación actual de la Carrera Informática, mediante la aplicación de técnicas de auditoría. • Identificar globalmente las actividades que se ejecutan en la Carrera Informática, para el desarrollo de la auditoría.		
	PROCEDIMIENTOS:		
1	Dialogar con los responsables de las áreas a examinar.	**P.T. 01**	Las autoras.
2	Visitar las instalaciones, para observar, inspeccionar y verificar el funcionamiento de las áreas a auditar.	**P.T. 02**	Las autoras.
3	Obtener la base legal de la entidad.	**P.T. 03**	Las autoras.
4	Obtener el organigrama estructural y funcional.	**P.T. 03**	Las autoras.
5	Verifique si la entidad ha elaborado y aprobado un plan estratégico.	**P.T. 03**	Las autoras.
6	Observar si la Carrera Informática preparó el plan operativo anual.	**P.T. 03**	Las autoras.
7	Verificar si existen manuales, políticas y procedimientos de operaciones.	**P.T. 03**	Las autoras.
8	Verificar si existen planes de contingencia.	**P.T. 03**	Las autoras.
	Conocer la estructura de los laboratorios,		

9	aulas y oficinas de la Carrera Informática.	**P.T. 04**	Las autoras
10	Solicitar información sobre los recursos tecnológicos disponibles, como documentos sobre los equipos, licencias, seguros, número de ellos, características, entre otros.	**P.T. 03**	Las autoras
11	Solicitar información sobre los sistemas instalados que contengan volúmenes de información.	**P.T. 03**	Las autoras
12	Dialogar con el director de la Carrera Informática los resultados de la planificación preliminar.	**P.T. 05**	Las autoras
13	Elaborar el Memorando de Planificación Preliminar.	**P.T. 05**	Las autoras

Elaborado por: Las autoras

ANEXO 4

CUESTIONARIOS DE CONTROL INTERNO PRELIMINARES

CARRERA DE INFORMÁTICA DE LA ESPAM MFL

CUESTIONARIO DE CONTROL INTERNO

Componente: Organización de la Entidad

ÁREA AUDITADA: DIRECCIÓN DE CARRERA			**FECHA:** 16/10/2013		
#	**PREGUNTAS**	**SI**	**NO**	**N/A**	**DETALLE**
1	¿La dirección desarrolla regularmente planes a corto, mediano y largo plazo que apoyen el logro de la misión y las metas generales de la organización?	X			Plan Anual Plan Operativo Rectorado académico
2	¿Dispone su institución de un plan Estratégico de Tecnología de Información?		X		
3	¿Durante el proceso de planificación, se presta adecuada atención al plan estratégico de la empresa?		X		
4	¿Las tareas y actividades en el plan tienen la correspondiente y adecuada asignación de recursos?			X	
5	¿Existe un comité de informática?		X		
6	¿Existen estándares de funcionamiento y procedimientos que gobiernen la actividad del área de informática por un lado y sus relaciones con los departamentos usuarios por otro?		X		
7	¿Existen estándares de funcionamiento y procedimientos y descripciones de puestos de trabajo adecuados y		X		

	actualizados?				
8	¿Los estándares y procedimientos existentes promueven una filosofía adecuada de control?			X	
9	¿Las descripciones de los puestos de trabajo reflejan las actividades realizadas en la práctica?		X		
10	¿Existen controles que tienden a asegurar que el cambio de puesto de trabajo y la finalización de los contratos laborales no afectan a los controles internos y a la seguridad informática?		X		
11	¿Existen procedimientos para la adquisición de bienes y servicios?	X			No están documentados, se envía oficio a Rectorado, para el plan operativo.
12	¿Existe un plan operativo anual?	X			
13	¿Cuentan con pólizas de seguros?	X			Dpto. Almacén
14	¿Existen procedimientos para vigilar y determinar permanentemente la legislación aplicable?			X	
15	¿Posee el inventario de los recursos tecnológicos que se utilizan en la carrera?	X			
TOTAL		**5**	**7**	**4**	
NOMBRE Y FIRMA DE ENTREVISTADO			**NOMBRE Y FIRMA DE ENTREVISTADOR**		

ANEXO 5

MEMORANDO DE PLANIFICACIÓN PRELIMINAR

CARRERA INFORMÁTICA

AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA A LOS RECURSOS DE TECNOLOGÍA DE INFORMACIÓN EN LA CARRERA INFORMÁTICA DE LA ESPAM MFL

Memorando de Planificación Preliminar

1. ANTECEDENTES

Debido al avance vertiginoso de la ciencia y la tecnología, los seres humanos necesitan conocer herramientas que les permitan realizar actividades con mayor agilidad para competir, en este mundo globalizado, con eficacia y eficiencia.

La ESPAM MFL, cuya misión es preparar al elemento humano, no puede ser la excepción y, como un ente integrador de las otras carreras que oferta, asume el compromiso de brindar una educación basada en la innovación tecnológica, a través del surgimiento de la Carrera de Informática.

2. MOTIVO DE LA AUDITORÍA

La auditoría de seguridad física y lógica a los recursos de tecnología de información en la Carrera Informática de la ESPAM MFL, se llevó a efecto como propuesta de tema de tesis que las autoras plantearon, la misma que tuvo autorización del ingeniero Leonardo Félix López, Rector de la ESPAM MFL, mediante el oficio Nº: ESPAM MFL –R – 2013 – 339 – OF, y la autorización del tribunal de tesis mediante el oficio S/N. de fecha 27 de agosto de 2013.

3. OBJETIVOS DE LA AUDITORÍA

- Comprobar la existencia de elementos que brinden salvaguarda a la infraestructura física de la carrera.

- Identificar controles de tecnologías de información.

- Verificar el nivel de cumplimiento de las políticas, planes y procedimientos que emplea la carrera en cuanto al uso de los recursos tecnológicos.

- Evaluar vulnerabilidades de una interrupción del servicio.

- Elaborar el Informe de Auditoría en la seguridad física y lógica considerando todos los hallazgos encontrados.

4. ALCANCE DEL EXAMEN

El proceso de Auditoría de Seguridad Física y Lógica se realizará en la Carrera Informática, en las áreas: de Dirección de Carrera, Secretaría, Desarrollo de Software, Mantenimiento y Soporte Técnico, Centro de Datos, Redes, Aulas, Laboratorios y otras dependencias involucradas.

5. CONOCIMIENTO DE LA ENTIDAD

5.1. Base Legal

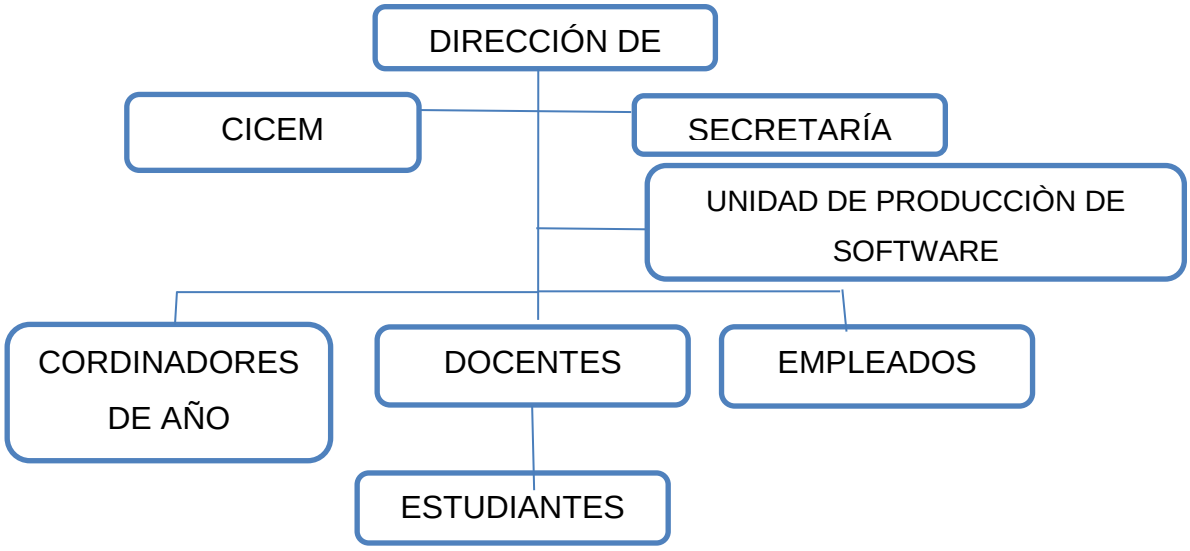
La Carrera Informática en la Escuela Superior Politécnica Agropecuaria de Manabí, se creó con el propósito de satisfacer la demanda de los estudiantes que ávidos de conocimientos, querían ingresar a esta carrera para obtener una profesión que les permitiera estar a la par con los avances de la ciencia y la tecnología.

Atendiendo lo dispuesto en la ley de creación de la Escuela Superior Politécnica Agropecuaria de Manabí – ESPAM, su Estatuto y Ley de Educación Superior, Consejo Politécnico de la ESPAM, el Ing. Leonardo Félix López rector de la ESPAM, informó al Presidente del CONESUP Ing. Vinicio Baquero Ordoñez que con fecha 16 de diciembre del 2002 se creó la carrera de Informática, con la modalidad presencial en los predios de la institución, localizada en el Cantón Bolívar - Provincia Manabí. En el mismo oficio se le acompañó el estudio correspondiente, característica de la carrera modalidad presencial, títulos: de Tecnólogos en Informática con seis semestres, y de Ingeniero en Informática con diez semestres, su diseño curricular centrado en el perfil profesional en coherencia con la Misión y Visión Institucional.

5.2. Disposiciones Legales

- Constitución Política de la República del Ecuador
- Ley Orgánica de Educación Superior
- Estatuto Orgánico de Gestión Organizacional por Procesos de la ESPAM MFL
- Reglamento Interno de la ESPAM MFL

5.3. Estructura Orgánica.



Elaborado por: Las autoras

5.4. Personal Laboral

NÓMINA DE DOCENTES
1. Q.F. Ana Aveiga Ortiz
2. Ing. Orlando Ayala Pullas
3. Ing. Lorena Carreño Mendoza
4. Ing. Luis Cedeño Valarezo
5. Lic. Bairo Cusme Cusme
6. Ing. Sergio Intriago Briones
7. Lic. Guillermo Intriago Cedeño
8. Dra. Isabel Matilla Blanco
9. Ing. Daniel Mera Martínez
10. Dr. José Montesdeoca Zambrano
11. Ing. Jéssica Morales Carrillo
12. Ing. Luis Ortega Arcia
13. Ing. Víctor Pinargote Bravo
14. Ing. Ángel Vélez Mero
15. Ing. Ricardo Vélez Valarezo
16. Lic. Maryury Zamora Cusme
17. Ing. Diego Toala Palma
18. Ing. Byron Camino Carlier
19. Ing. Gustavo Molina Garzón
20. Lic. Edys Solórzano Intriago
21. Ing. Joffre Moreira Pico

Fuente: Secretaría de Carrera de Informática

5.5. Objetivos de la Carrera Informática.

El profesional en informática se forma para solucionar problemas de software-hardware y dirigir aspectos inherentes a esta actividad en cualquier empresa e institución con espíritu crítico y humanista.

5.5.1. Objetivos Educativos:

- Preparar profesionales eficientes y con sólidos conocimientos científicos comprometidos con las condiciones sociales, económicas y ambientales del país, capaces de introducir y desarrollar la cultura a través de sistemas informáticos.

- Proveer profesionales informáticos con capacitación integral que les permita adaptarse a las TIC's de un mundo globalizado.

5.5.2. Objetivos Instructivos:

- Desarrollar sistemas informáticos de hardware o software para la solución eficiente y eficaz de problemas de procesamiento automático de datos y de información.

- Manejar las herramientas de software de última tecnología en el ámbito de su profesión que se encuentren en el mercado.

- Implementar redes y sistemas de comunicación con su respectivo soporte.

- Brindar mantenimiento preventivo y correctivo a diferentes equipos y sistemas computacionales en instituciones y empresas públicas y privadas.

- Participar en proyectos de investigación, desarrollo y automatización tecnológica.

- Cursar programas de posgrado o de formación continua en áreas afines.

5.6. Misión y Visión

5.6.1. Misión.

Formación de Profesionales íntegros que conjuguen ciencia, tecnología y valores en su accionar, comprometidos con la comunidad en el manejo adecuado de programas y herramientas computacionales de última generación

5.6.2. Visión

Ser referentes en la formación de profesionales de prestigio en el desarrollo de aplicaciones informática y soluciones de hardware.

5.7. Descripción estructural de la carrera

La carrera de Informática, se encuentra ubicada en el Campus Politécnico, km 2.7 vía Calceta – El Morro – El Limón, Manabí, Ecuador, actualmente cuenta con una Dirección de Carrera, la que posee como dependencia a la Unidad de Producción de Software UPS y Mantenimiento de Equipos, la carrera internamente aún no cuenta con un organigrama estructural definido legalmente y por ende con un manual de funciones, sólo la dirección de carrera tiene definidas sus funciones en el Estatuto Orgánico de Gestión Organizacional por Procesos de la ESPAM MFL.

La edificación de la carrera, posee tres plantas en la baja está compuesta por tres laboratorios: el de electrónica, los cubículos de docentes de tiempo completo, la sala de docentes a medio tiempo, la sala de coordinadores de año, el auditorio de la carrera, el Centro de Datos que almacena la información de toda la universidad.

En la primer planta existen un laboratorio y dos aulas habilitadas y cuatro habilitándose, adicionalmente se encuentra ubicada la oficina de la Unidad de Producción de Software UPS, la dirección de carrera, la oficina de la secretaría de la carrera y la oficina del director del Centro de Aplicaciones Informáticas CAI, los estudiantes de este centro reciben clases en los laboratorios de la carrera.

En la segunda planta se encuentra, cuatro aulas habilitadas y dos por habilitarse.

La dependencia de mantenimiento de equipos no funciona en las instalaciones de la carrera, esta dependencia, ofrece sus servicios a toda la Politécnica de Manabí.

5.8. Funciones y actividades que realiza Dirección de carrera

(Estatuto orgánico de gestión organizacional por procesos. 2012) Dirigir, coordinar, organizar y evaluar las actividades administrativas, académicas, investigativas de la carrera de informática.

Atribuciones y responsabilidades:

- Dirigir, planificar, ejecutar y evaluar las actividades académicas, administrativas, de investigación y vinculación de la carrera;
- Coordinar el desarrollo de la investigación formativa y generativa, en base a los lineamientos de la ESPAM MFL;
- Gestionar las soluciones a las necesidades de la Carrera, frente a la autoridad correspondiente;
- Convocar y presidir la asamblea de profesores de la carrera y comisiones creadas para distintos fines;
- Delegar a los profesores las distintas comisiones curriculares y extracurriculares;
- Representar al cuerpo docente ante la consejo académico;
- Coordinar las actividades desarrolladas en laboratorios y unidades académicas, investigación y vinculación a cargo;
- Gestionar las solicitudes de orden académico, realizadas por los estudiantes y docentes de la carrera
- Informar a la autoridad correspondiente, sobre el avance y desarrollo de las actividades académicas, administrativas, de investigación y vinculación con la carrera.
- Cumplir y hacer cumplir las disposiciones de la LOES su Reglamento y más disposiciones emanadas por las máximas autoridades de la ESPAM MFL.

Actualmente la Dirección realiza además de sus funciones encomendadas para la carrera, se encargada de la provisión y administración de los servicios informáticos, comunicaciones e implantación de la infraestructura tecnológica de la ESPAM MFL. La UPS ubicada en el edifico de Informática fue creada en el 2003 y surge de la necesidad de aplicaciones en la Politécnica de Manabí, en la ejecución del avance de sus desarrollos no poseen procedimientos estandarizados.

5.9. Descripción y características de los recursos tecnológicos disponibles

La carrera de Informática, en el inventario que realizaron las autoras, posee:

Nº	Recursos de la carrera
AULAS Y LABORATORIOS	
76	Computadoras de escritorio
10	Proyectores
10	Amplificadores
10	Sensores de humo
13	Cámaras
33	Puntos de conexión a red

6. PUNTOS DE INTERES PARA LA AUDITORÍA

- Definir el porcentaje de seguridad de los recursos tecnológicos.
- Determinar el cumplimiento de políticas, normas y manuales en la ejecución de la misión, visión y objetivos de la carrera.

7. IDENTIFICACIÓN DE LOS COMPONENTES A SER EXAMINADOS EN LA PLANIFICACIÓN ESPECÍFICA

Los componentes a evaluar son:

- Gestión de Software y aplicaciones
- Protección de los Activos Informáticos
- Protección de la Información
- Gestión del mantenimiento de Software y Hardware
- Gestión del Data Center

ANEXO 6

PROGRAMA ESPECÍFICO DE AUDITORÍA

CARRERA INFORMÁTICA

AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA A LOS RECURSOS DE TECNOLOGÍA DE INFORMACIÓN EN LA CARRERA INFORMÁTICA DE LA ESPAM MFL

PROGRAMA GENERAL PARA LA PLANIFICACIÓN ESPECÍFICA

Nº	OBJETIVOS:	REFERENCIA	ELABORADO POR:
	• Evaluar el control interno a la entidad, verificando sus puntos fuertes y débiles. • Determinar el nivel de riesgo y confianza del ambiente informático de la entidad.		
	PROCEDIMIENTOS		
1	Desarrollar cuestionarios de control interno para los componentes determinados en la planificación preliminar (Gestión de Activos, Protección de la Información, Data Center, Mantenimiento de Software y Hardware y Desarrollo de Software.	**P.T. 06**	Las autoras
2	Aplicar cuestionarios de control interno, a los responsables de las áreas involucradas en la auditoría.	**P.T. 06**	Las autoras
3	Evaluar el control interno.	**P.T. 07**	Las autoras
4	Elaborar las matrices de riesgo confianza por cada componente.	**P.T. 07**	Las autoras
5	Elaborar hallazgos de auditoría, según la evaluación de Control Interno.	**P.T. 08**	Las autoras
6	Obtener los programas de auditoría a la medida por cada componente.	**P.T. 10**	Las autoras
7	Dialogar con el director de la Carrera Informática los resultados de la planificación preliminar.	**P.T. 11**	Las autoras

8	Preparar un Memorando de Planificación Específica con el resultado del trabajo, las conclusiones alcanzadas y los comentarios acerca de la solidez y/o debilidades de control interno que requieren tomar una acción inmediata o puedan ser puntos apropiados para nuestra carta de observaciones y recomendaciones.	**P.T. 11**	Las autoras

Elaborado por: Las autoras

ANEXO 7

MEMORANDO DE PLANIFICACIÓN ESPECÍFICA

CARRERA INFORMÁTICA

AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA A LOS RECURSOS DE TECNOLOGÍA DE INFORMACIÓN EN LA CARRERA INFORMÁTICA DE LA ESPAM MFL

MEMORÁNDO DE PLANIFICACIÓN ESPECÍFICA

1. REFERENCIA DE LA PLANIFICACION PRELIMINAR

La planificación preliminar a la Carrera Informática de la ESPAM MFL, de la ciudad de Calceta, se entregó el 02 de Octubre de 2013 en la que se estableció el enfoque de la auditoria para la planificación especifica; como se observó en la planificación preliminar la entidad cuenta con lineamientos generales respecto a la seguridad informática, así mismo, no se deja evidencia documentada de los procesos de control y utilización de los recursos tecnológicos, por ello se sugirió que las pruebas de cumplimiento se revisen en forma más clara, a fin de determinar las causas por las que la entidad no cumple con las disposiciones establecidas en las Normas de Control Interno.

2. OBJETIVOS POR AREAS O COMPONENTES

Los componentes seleccionados para esta evaluación corresponde a: Seguridad del Data Center, Protección de los Activos Tangibles, Protección de los Activos Intangibles, Gestión de Mantenimiento de Hardware y Software, y Gestión de Desarrollo de Software, los cuales tiene como objetivo: Identificar las medidas de seguridad aplicadas respecto a cada componente, es decir:

- Identificar las medidas de seguridad implantadas Seguridad del Data Center.
- Identificar las medidas de seguridad implantadas Protección de los Activos Tangibles.
- Identificar las medidas de seguridad implantadas Protección de los Activos Intangibles.
- Identificar las medidas de seguridad implantadas Gestión de Mantenimiento de Hardware y Software.

- Identificar las medidas de seguridad implantadas Desarrollo de Software.

Cuadro 1. Matriz general porcentual del nivel de Riesgo-Confianza
Fuente: Cuestionarios de Control Interno

3. RESULTADO DE LA EVALUACION DE CONTROL INTERNO

MATRIZ DE RIESGO-CONFIANZA

Data Center		Activos Tangibles		Activos Intangibles		Mantenimiento		Gestión Desarrollo de Software	
Riesgo	Confianza	Riesgo	Confianza	Riesgo	Confianza	Riesgo	Confianza	Riesgo	Confianza
37,50%	62,50%	43,75%	56,25%	32,15%	67,85%	55,89%	44,11%	50%	50%

La evaluación de control Interno efectuada a la Carrera Informática, dio como resultado varias debilidades en los componentes anteriormente señalados, de los cuales se puede detallar de forma abreviada los niveles de riesgo y confianza:

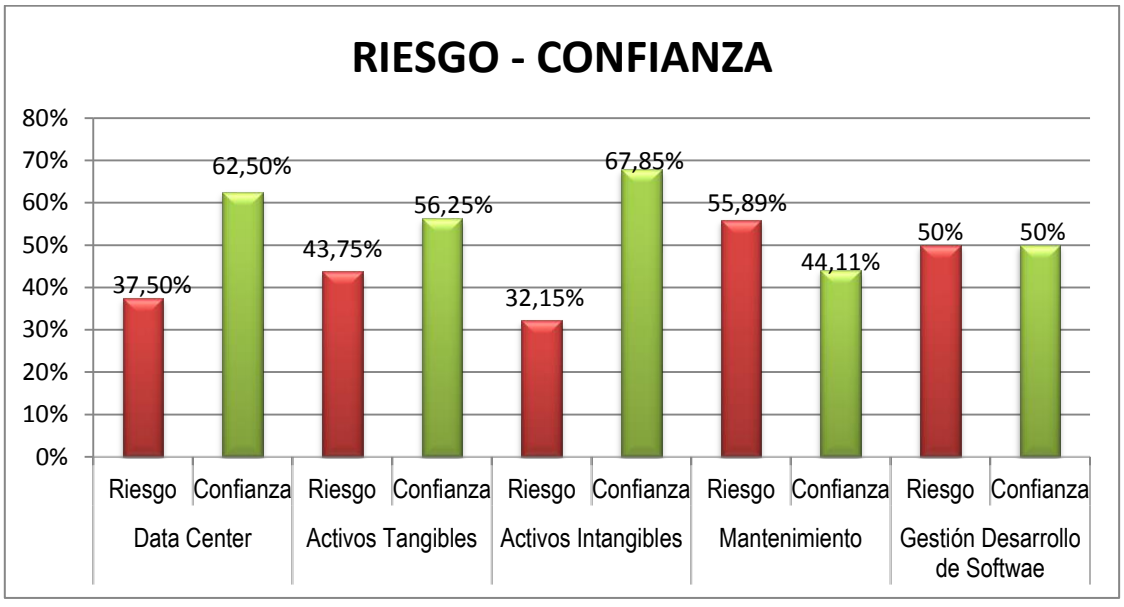


Gráfico 2. Nivel porcentual del Riesgo Confianza en la Carrera Informática

Se observa que en el Data Center, el nivel de confianza sobre medidas de seguridad es de 62,50% frente a la proporcionalidad de riesgo de 37,50%; sobre la protección de Activos Tangibles en la Carrera tiene un nivel de confianza de 56,25% y la proporción de riesgo es de 43,75%; en la protección de Activos Intangibles el porcentaje de

confianza es de 67,85%, ante un porcentaje proporcional de 32,15%; en la gestión de Mantenimiento, el 44,11% corresponde a la confianza y el 55,89% es de riesgo; y en la Gestión de Desarrollo de Software, el nivel de confianza es de 50%, y el riesgo es 50%.

Es así, que se evidencia que el sector con mayor nivel de confianza es la protección de los Activos Intangibles con una confianza de 67,85 y el componente con menor nivel de confianza es la gestión de mantenimiento con 44,11%.

4. EVALUACION Y CALIFICACION DE LOS RIESGOS

De conformidad a la evaluación del control interno a los componentes seleccionados los resultados son los siguientes:

Cuadro 3. Matriz de resultados de nivel de Riesgo-Confianza

COMPONENTE	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO
Seguridad del Data Center	62, 50%	MODERADO	MODERADO
Protección de Activo Intangibles	56,25%	MODERADO	MODERADO
Protección de Activos Tangibles	67,85%	MODERADO	MODERADO
Gestión de Mantenimiento de Hardware y Software	44,11%	BAJO	ALTO
Desarrollo de Software	50%	BAJO	ALTO

5. COEFICIENTE DE CONCORDANCIA DE KENDALL

Cuadro 4. Concordancia de preguntas similares de los Cuestionarios Aplicados

Ítem K	Preguntas	Director de Carrera	Administración de Data center y Redes	Asistencia de TIC	Coordinador de UPS	∑aij	A	A^2
1	Existencia de Políticas de Seguridad documentadas.	4	4	3	4	15	5	25
2	Existencia de mecanismos de acceso físico al área.	2	1	2	2	7	-3	9
3	Existencia de registro de entrada y salida de recursos tecnológicos.	3	3	4	3	13	3	9
4	Existencia documentada de las funciones y responsabilidades en las áreas.	1	2	1	1	5	-5	25
						40		**68**

Cuadro 4.13. Remplazo de fórmulas para Coeficiente de Concordancia de Kendall.

Determinar valor de A:	Determinar el valor de T:
$A = \sum aij - T$ $A = 15 - 10$ $A = 5$ Para la primera pregunta, y así hasta culminar.	$T = \frac{\sum aij}{K}$ $T = \frac{40}{4}$ $T = 10$

Remplazo de la fórmula

$$w = \frac{12\sum A^2}{n^2\ 4(k^2 - 1)}$$

$$w = \frac{12(68)}{4^2\ 4(4^2 - 1)}$$

$$w = 0{,}85$$

Con el dato obtenido, se concluye que el grado de coincidencia de las respuestas equivale a 0,85 determinando que existen concordancia en los resultados, por lo tanto se afirma que la entidad auditada, cuenta con un bajo control documentado, de políticas aprobadas, de registros de entrada y/o salida de los recursos tecnológicos, y concuerdan además que sus funciones y responsabilidades son conocidas, y que se han tomado lineamientos generales de seguridad en las áreas.

6. PROGRAMA DE AUDITORIA

Los programas de auditoría de la presente evaluación a los componentes establecidos de la Carrera Informática, se desarrollaron en base al conocimiento de riesgos presentados, se utilizó pruebas de cumplimiento, que permitan alcanzar el objetivo en cada uno de los componentes, sustentar nuestros hallazgos, conclusiones y recomendaciones.

7. DISTRIBUCIÓN DE TIEMPO, TALENTO HUMANO, RECURSOS MATERIALES Y FINANCIEROS

RESPONSABLE	ACTIVIDADES	TIEMPO / DÍAS
Autoras	Planificación y programación	40
	Análisis de información	20
	Revisión P/T comentarios conclusiones	
	Y recomendaciones	15
	Comunicación parcial de resultados	5
	Elaboración borrador de informe	10
		90

8. RECURSOS A UTILIZARSE

8.1 MATERIALES

En el transcurso de la auditoría se utilizaran los siguientes materiales:

Cantidad	Detalle
2	Computadora
2	Resma de papel A4
1	Tinta para la impresora
5	Cuaderno de notas
5	3 esferos negros y 2 esferos azules
5	Lápiz mecánicos
5	Borrador
5	Carpeta
5	Resaltado
5	Corrector

8.2 FINANCIEROS

NOMBRES Y APELLIDOS	TIEMPO/ DÍAS	SUBSISTENCIA	MOVILIZACIÓN	TOTAL
Verónica Espinoza	90	$ 100,00	$ 80,00	$ 180
Amarilis Loor	90	$ 100,00	$ 80,00	$ 180
1 TOTAL		$ 200,00	$ 160,00	$ 360

8.3. PRODUCTO A OBTENER

Como resultado de la auditoría de seguridad física y lógica a los recursos de tecnología de información en la carrera Informática de la ESPAM MFL, se obtendrá como resultado el informe final.

ANEXO 8

PROGRAMA DE AUDITORÍA POR COMPONENTES

CARRERA INFORMÁTICA

AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA A LOS RECURSOS DE TECNOLOGÍA DE INFORMACIÓN EN LA CARRERA INFORMÁTICA DE LA ESPAM MFL

PROGRAMA PARA LA SEGURIDAD DEL DATA CENTER

N°	OBJETIVO	REFERENCIA	HECHO POR
	• Identificar las medidas de seguridad implantadas para la seguridad del Data Center.		
	PRUEBAS DE CUMPLIMIENTO		
1	Verificar si existen medidas seguridad físicas tales como: control de accesos, piso elevados o protegidos, controles de humedad, control de temperatura, fuente interrumpida de energía, dispositivos de detección de agua, detectores de humo y un sistema adecuado de extinción de incendios.	**P.T. 12**	Las autoras
2	Verificar la existencia de protección contra variaciones de voltaje a toda la potencia eléctrica que se suministra a la unidad central de proceso y al equipo de comunicación.	**P.T.13**	Las autoras
3	Verificar la existencia de planos de Data Center, diagramas de cableado eléctrico, diagramas de red, diagramas de ductos e inventarios de software y software.	**P.T. 14**	Las autoras
4	Dialogar con el responsable para identificar si conocen las responsabilidades que tienen asignadas en una situación de desastre.	**P.T. 15**	Las autoras

5	Verificar la existencia del plan de contingencia y si este hace referencia a normas y políticas establecidas.	**P.T. 16**	Las autoras
6	Verificar mediante entrevistas que el personal involucrado tiene conocimiento de los procedimientos a seguir para la continuidad de las operaciones en caso de desastres.	**P.T. 17**	Las autoras
7	Verificar si existe vigilancia en el área las 24 horas.	**P.T. 18**	Las autoras

Elaborado por: Las autoras

CARRERA INFORMÁTICA

AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA A LOS RECURSOS DE TECNOLOGÍA DE INFORMACIÓN EN LA CARRERA INFORMÁTICA DE LA ESPAM MFL

PROGRAMA DE AUDITORÍA PARA LA PROTECCIÓN DE ACTIVOS TANGIBLES

N°	OBJETIVOS:	REFERENCIA	HECHO POR
	• Identificar las medidas de seguridad implantadas Protección de los Activos Tangibles.		
	PRUEBAS DE CUMPLIMIENTO		
1	Verificar si existen políticas de seguridad informática, para la protección de los recursos tecnológicos.	**P.T. 19**	Las autoras
2	Verificar si se dispone de los planos del edificio, con la finalidad de visualizar su distribución para identificar riesgos para el equipo informático.	**P.T. 20**	Las autoras
3	Solicitar planes de mantenimiento de los recursos tecnológicos que se utilizan en la carrera.	**P.T. 21**	Las autoras
4	Verificar que medidas de control utilizan en caso de extravío de algún dispositivo.	**P.T 22.**	Las autoras
5	Solicitar, las pólizas de seguros de los recursos tecnológicos.	**P.T. 23**	Las autoras
6	Garantías obtenidas en la adquisición de los recursos tecnológicos.	**P.T. 24**	Las autoras
7	Solicitar manuales y guías sobre soportes de los equipos tecnológicos.	**P.T. 25**	Las autoras

8	Verifique si la entidad ha elaborado un inventario de los recursos tecnológicos y de extintores, extinguidores y sensores de humo.	P.T. 26	Las autoras
9	Verificar controles de acceso a las instalaciones de la carrera.	P.T. 27	Las autoras
10	Verificar la existencia de sistemas de vigilancia en la edificación	P.T. 28	Las autoras
11	Verificar controles de ingreso y salida de los recursos tecnológicos.	P.T. 29	Las autoras

Elaborado por: Las autoras

CARRERA INFORMÁTICA

AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA A LOS RECURSOS DE TECNOLOGÍA DE INFORMACIÓN EN LA CARRERA INFORMÁTICA DE LA ESPAM MFL

PROGRAMA PARA LA PROTECCIÓN DE ACTIVOS INTANGIBLES

N°	OBJETIVOS:	REFERENCIA	HECHO POR
	• Identificar las medidas de seguridad implantadas Protección de los Activos Intangibles.		
	PRUEBAS DE CUMPLIMIENTO		
1	Verificar la existencia de políticas de seguridad para medir riesgos y amenazas.	P.T. 30	Las autoras
2	Constatar si existen mecanismos para el acceso a información confidencial y protección de datos.	P.T. 31	Las autoras
3	Verificar el monitoreo de las actividad de los usuarios, administrativos y operativos a fin de detectar y corregir desviaciones en el uso correcto de la información, o en el cumplimiento de procedimientos asociados a la seguridad de la información.	P.T. 32	Las autoras
4	Verificar la existencia de controles sobre reserva y confidencialidad de la información.	P.T. 33	Las autoras
5	Verificar los mecanismos adoptados para la identificación y autenticación de usuarios en la red, para garantizar la legitimidad de las operaciones que estos realizan.	P.T. 34	Las autoras
6	Verificar que mecanismos se utilizan	P.T. 35	Las autoras

	para prevenir probables intrusiones.		
7	Verificar si los usuarios no pueden acceder a ningún sistema, sin antes haberse autenticado correctamente en la red institucional.	P.T. 36	Las autoras
8	Verificar si se inhabilita al usuario después de ingresar la contraseña un número determinado de intentos fallidos.	P.T. 37	Las autoras
9	Verificar que las contraseñas no sean mostradas en pantalla cuando se ingresan.	P.T. 38	Las autoras
10	Verificar si durante el proceso de identificación, los usuarios son informados de cuando fue su última conexión, para ayudar a identificar potenciales suplantaciones o accesos no autorizados.	P.T. 39	Las autoras
11	Verificar si existen políticas que incluyen el uso de software para la detección de virus, y los mecanismos usados para la actualización.	P.T. 40	Las autoras
12	Verificar si existen procedimientos para la administración de los Firewall para prevenir el acceso no autorizado a la red interna.	P.T. 41	Las autoras
13	Verificar el proceso que utiliza la entidad para detectar y prevenir virus.	P.T. 42	Las autoras
14	Verificar las herramientas de autenticación.	P.T. 43	Las autoras
15	Verificar quienes son los responsables de la administración del sistema biométrico.	P.T. 44	Las autoras

Elaborado por: Las autoras

CARRERA INFORMÁTICA

AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA A LOS RECURSOS DE TECNOLOGÍA DE INFORMACIÓN EN LA CARRERA INFORMÁTICA DE LA ESPAM MFL

PROGRAMA DE AUDITORÍA PARA MANTENIMIENTO DE HARDWARE Y SOFTWARE

N°	OBJETIVOS:	REFERENCIA	HECHO POR
	• Identificar las medidas de seguridad implantadas para la seguridad en el mantenimiento de hardware y software.		
	PRUEBAS DE CUMPLIMIENTO		
1	Verificar la existencia de políticas para dar mantenimiento a los recursos tecnológicos.	P.T. 45	Las autoras
2	Constatar la existencia de inventarios de los equipos a los que se les da mantenimiento.	P.T. 46	Las autoras
3	Verificar cual es el proceso de notificación de las fallas del equipo informático y como se documenta dicho proceso.	P.T. 47	Las autoras
4	Verificar si se les da mantenimiento a todos los equipos de la carrera o solo una parte específica.	P.T. 48	Las autoras
5	Constatar la existencia de historial de solicitudes de cambios o actualizaciones de los sistemas.	P.T. 49	Las autoras
6	Constatar la existencia de planes de mantenimiento preventivo.	P.T. 50	Las autoras
7	Solicitar planes de mantenimiento de los sistemas, software, aplicaciones utilizados en la carrera.	P.T. 51	Las autoras
8	Solicitar las licencias y actualizaciones de las aplicaciones, sistemas, software implementados.	P.T. 52	Las autoras
9			

Elaborado por: Las autoras

CARRERA INFORMÁTICA

AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA A LOS RECURSOS DE TECNOLOGÍA DE INFORMACIÓN EN LA CARRERA INFORMÁTICA DE LA ESPAM MFL

PROGRAMA DE AUDITORÍA PARA LA GESTIÓN DE SOFTWARE Y APLICACIONES

N°	OBJETIVOS:	REFERENCIA	HECHO POR
	• Identificar las medidas de seguridad implantadas para la Unidad de Producción de Software.		
	PRUEBAS DE CUMPLIMIENTO		
1	Verificar la existencia de medidas, procedimientos definidos en una normativa de seguridad.	P.T. 53	Las autoras
2	Verificar el control de acceso a la unidad	P.T. 54	Las autoras
3	Constatar si se actualizan, las aplicaciones para evitar, sustracción de información, como antivirus, firewall, entre otros	P.T. 55	Las autoras
4	Verificar si se registran los ingresos o salida de sus equipos tecnológicos a la unidad.	P.T. 56	Las autoras

Elaborado por: Las autoras

ANEXO 9

INFORME FINAL DE AUDITORÍA

INFORME FINAL

AUDITORÍA DE SEGURIDAD FÍSICA Y LÓGICA A LOS RECURSOS DE TECNOLOGÍA DE INFORMACIÓN EN LA CARRERA INFORMÁTICA DE LA ESPAM MFL

CARTA DE PRESENTACIÓN

Calceta, 17 de febrero de 2014

Ing. Luis Cedeño
DIRECTOR DE LA CARRERA INFORMÁTICA DE LA ESPAM MFL
Ciudad.-

De mi consideración:

Se ha realizado la Auditoría de Seguridad Física y Lógica a los Recursos de Tecnología de Información en la Carrera Informática de la ESPAM MFL, por el período comprendido entre el 30 de septiembre de 2013 hasta el 28 de febrero de 2014.

Nuestra acción de control se efectuó de acuerdo con las Normas Ecuatorianas de Auditoría Gubernamental emitidas por la Contraloría General del Estado. Estas normas requieren que la auditoría sea planificada y ejecutada para obtener 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 con las disposiciones legales y reglamentarias vigentes, políticas y demás normas aplicables.

Debido a la naturaleza de la acción de control efectuada, los resultados se encuentran expresados en las conclusiones y recomendaciones que constan en el presente informe. Una adecuada implantación de aquello, permitirá mejorar los procedimientos para la gestión de los recursos tecnológicos de la entidad.

Atentamente,

Verónica Espinoza Castillo Amarilis Loor Párraga

CAPÍTULO I

INFORMACIÓN INTRODUCTORIA

MOTIVO DE LA AUDITORÍA

La auditoría de seguridad física y lógica a los recursos de tecnología de información en la Carrera Informática de la ESPAM MFL, se llevó a efecto como propuesta de tema de tesis que las autoras plantearon, la misma que tuvo autorización del ingeniero Leonardo Félix López, Rector de la ESPAM MFL, mediante el oficio Nº: ESPAM MFL –R – 2013 – 339 – OF, y la autorización del tribunal de tesis mediante el oficio S/N. de fecha 27 de agosto de 2013.

OBJETIVOS DE LA AUDITORÍA

- Comprobar la existencia de elementos que brinden salvaguarda a la infraestructura física de la carrera.

- Identificar controles de tecnologías de información.

- Verificar el nivel de cumplimiento de las políticas, planes y procedimientos que emplea la carrera en cuanto al uso de los recursos tecnológicos.

- Evaluar vulnerabilidades de una interrupción del servicio.

- Elaborar el informe de auditoría en la seguridad física y lógica considerando todos los hallazgos encontrados.

ALCANCE DEL EXAMEN

El proceso de Auditoría de Seguridad Física y Lógica se realizará en la Carrera Informática, en las áreas: de Dirección de Carrera, Secretaría, Desarrollo de Software, Mantenimiento y Soporte Técnico, Centro de Datos, Redes, Aulas, Laboratorios y otras dependencias involucradas.

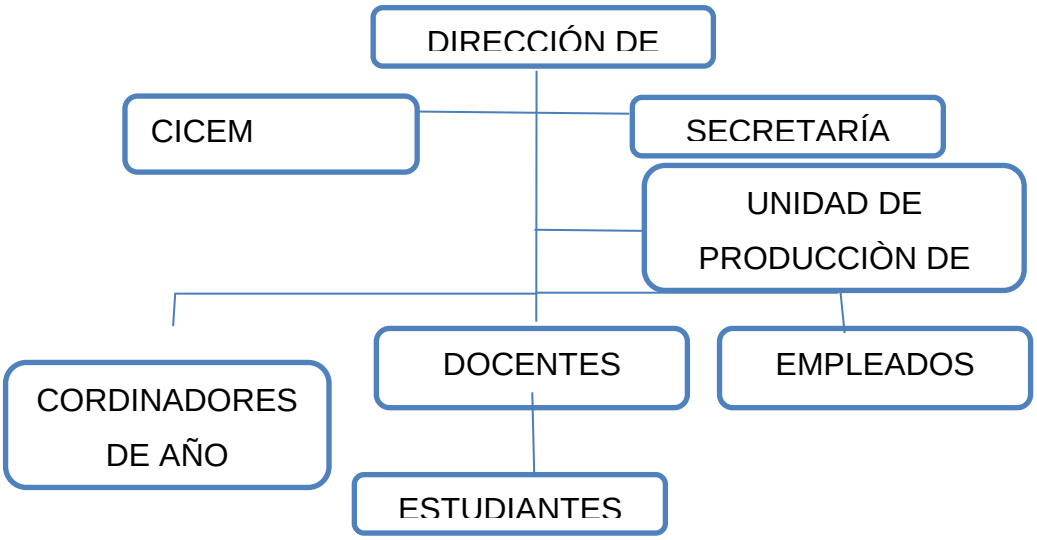
BASE LEGAL

Atendiendo lo dispuesto en la ley de creación de la Escuela Superior Politécnica Agropecuaria de Manabí – ESPAM, su Estatuto y Ley de Educación Superior, Consejo Politécnico de la ESPAM, el Ing. Leonardo Félix López rector de la ESPAM, informó al Presidente del CONESUP Ing. Vinicio Baquero Ordoñez que con fecha 16 de diciembre del 2002 se creó la carrera de Informática, con la modalidad presencial en los predios de la institución, localizada en el Cantón Bolívar - Provincia Manabí. En el mismo oficio se le acompañó el estudio correspondiente, característica de la carrera modalidad presencial, títulos: de Tecnólogos en Informática con seis semestres, y de Ingeniero en Informática con diez semestres, su diseño curricular centrado en el perfil profesional en coherencia con la Misión y Visión Institucional.

DISPOSICIONES LEGALES

- Constitución Política de la República del Ecuador
- Ley Orgánica de Educación Superior
- Estatuto Orgánico de Gestión Organizacional por Procesos de la ESPAM MFL
- Reglamento Interno de la ESPAM MFL

ESTRUCTURA ORGÁNICA



Elaborado por: Las autoras

OBJETIVOS DE LA CARRERA INFORMÁTICA

El profesional en informática se forma para solucionar problemas de software-hardware y dirigir aspectos inherentes a esta actividad en cualquier empresa e institución con espíritu crítico y humanista.

7.1.1. Objetivos Educativos:

- Preparar profesionales eficientes y con sólidos conocimientos científicos comprometidos con las condiciones sociales, económicas y ambientales del país, capaces de introducir y desarrollar la cultura a través de sistemas informáticos.
- Proveer profesionales informáticos con capacitación integral que les permita adaptarse a las TIC’s de un mundo globalizado.

7.1.2. Objetivos Instructivos:

- Desarrollar sistemas informáticos de hardware o software para la solución eficiente y eficaz de problemas de procesamiento automático de datos y de información.

- Manejar las herramientas de software de última tecnología en el ámbito de su profesión que se encuentren en el mercado.

- Implementar redes y sistemas de comunicación con su respectivo soporte.

- Brindar mantenimiento preventivo y correctivo a diferentes equipos y sistemas computacionales en instituciones y empresas públicas y privadas.

- Participar en proyectos de investigación, desarrollo y automatización tecnológica.

- Cursar programas de posgrado o de formación continua en áreas afines.

CAPÍTULO II

RESULTADO DE LA EVALUACION DE CONTROL INTERNO

La evaluación de control Interno efectuada a la Carrera Informática, dio como resultado varias debilidades en los componentes anteriormente señalados, de los cuales se puede detallar de forma abreviada los niveles de riesgo y confianza:

Cuadro 1. Matriz general porcentual del nivel de Riesgo-Confianza

MATRIZ DE RIESGO-CONFIANZA

Data Center		**Activos Tangibles**		**Activos Intangibles**		**Mantenimiento**		**Gestión Desarrollo de Software**	
Riesgo	Confianza	Riesgo	Confianza	Riesgo	Confianza	Riesgo	Confianza	Riesgo	Confianza
37,50%	62,50%	43,75%	56,25%	32,15%	67,85%	55,89%	44,11%	50%	50%

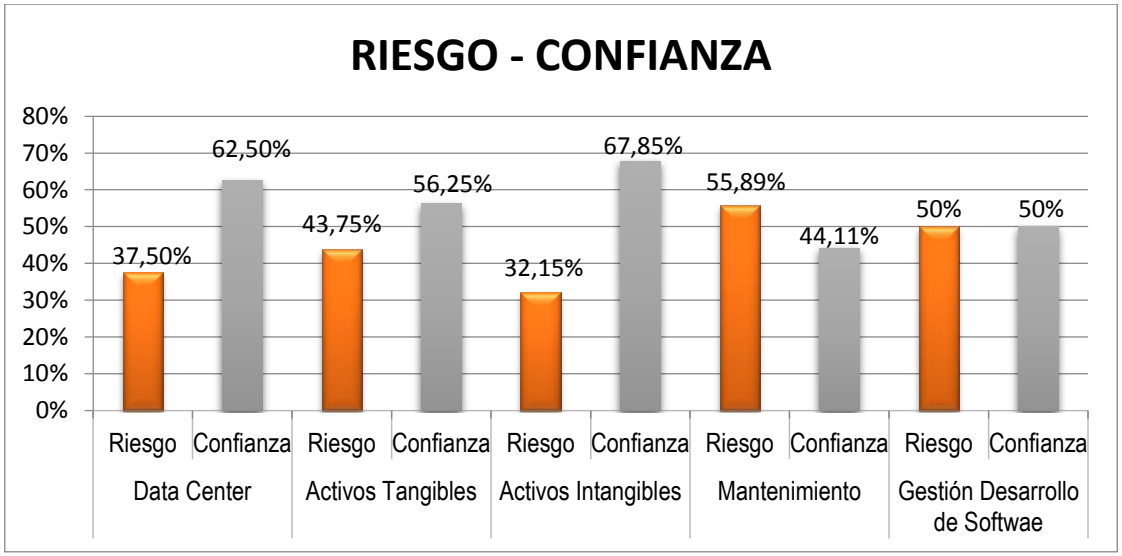


Gráfico 2. Nivel porcentual del Riesgo Confianza en la Carrera Informática

Se observa que en el Data Center, el nivel de confianza sobre medidas de seguridad es de 62,50% frente a la proporcionalidad de riesgo de 37,50%; sobre la protección de Activos Tangibles en la Carrera tiene un nivel de confianza de 56,25% y la proporción de riesgo es de 43,75%; en la protección de Activos Intangibles el porcentaje de confianza es de 67,85%, ante un porcentaje proporcional de 32,15%; en la gestión de Mantenimiento, el 44,11% corresponde a la confianza y el 55,89% es de riesgo; y en la Gestión de Desarrollo de Software, el nivel de confianza es de 50%, y el riesgo es 50%.

Es así, que se evidencia que el sector con mayor nivel de confianza es la protección de los Activos Intangibles con una confianza de 67,85 y el componente con menor nivel de confianza es la gestión de mantenimiento con 44,11%.

EVALUACION Y CALIFICACION DE LOS RIESGOS

De conformidad a la evaluación del control interno a los componentes seleccionados los resultados son los siguientes:

Cuadro 3. Matriz de resultados de nivel de Riesgo-Confianza

COMPONENTE	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO
Seguridad del Data Center	62, 50%	MODERADO	MODERADO
Protección de Activo Intangibles	56,25%	MODERADO	MODERADO
Protección de Activos Tangibles	67,85%	MODERADO	MODERADO
Gestión de Mantenimiento de Hardware y Software	44,11%	BAJO	ALTO
Desarrollo de Software	50%	BAJO	ALTO

COEFICIENTE DE CONCORDANCIA DE KENDALL

Cuadro 4. Concordancia de preguntas similares de los Cuestionarios Aplicados

Ítem K	Preguntas	Director de Carrera	Administración de Data center y Redes	Asistencia de TIC	Coordinador de UPS	∑aij	A	A^2
1	Existencia de Políticas de Seguridad documentadas.	4	4	3	4	15	5	25
2	Existencia de mecanismos de acceso físico al área.	2	1	2	2	7	-3	9
3	Existencia de registro de entrada y salida de recursos tecnológicos.	3	3	4	3	13	3	9
4	Existencia documentada de las funciones y responsabilidades en las áreas.	1	2	1	1	5	-5	25
						40		**68**

Cuadro 5. Remplazo de fórmulas para Coeficiente de Concordancia de Kendall.

Determinar valor de A:	**Determinar el valor de T:**
$A = \sum aij - T$ $A = 15 - 10$ $A = 5$ Para la primera pregunta, y así hasta culminar.	$T = \frac{\sum aij}{K}$ $T = \frac{40}{4}$ $T = 10$

Remplazo de la fórmula

$$w = \frac{12\sum A^2}{n^2\ 4(k^2 - 1)}$$

$$w = \frac{12(68)}{4^2\ 4(4^2 - 1)}$$

$$w = 0{,}85$$

Con el dato obtenido, se concluye que el grado de coincidencia de las respuestas equivale a 0,85 determinando que existen concordancia en los resultados, por lo tanto se afirma que la entidad auditada, cuenta con un bajo control documentado, de políticas aprobadas, de registros de entrada y/o salida de los recursos tecnológicos, y concuerdan además que sus funciones y responsabilidades son conocidas, y que se han tomado lineamientos generales de seguridad en las áreas.

CAPÍTULO III

HALLAZGOS Y RECOMENDACIONES

DETECCIÓN DE HALLAZGOS		
ÁREA	**RESPONSABLE**	**ORIGEN**
Carrera Informática	**Director de Carrera**	**AUDITORÍA TECNOLÓGICA**

2 BASE LEGAL:	***Norma de Control Interno 410*** titulada ***Tecnología de la Información,*** referente a la ***410-04 Políticas y procedimientos.***
PROCEDIMIENTO	Verificar la existencia de políticas o procedimientos legalmente aprobados y documentados, que permitan regular las actividades de seguridad, acceso y/o control interno.
CONDICIÓN	De acuerdo a la evaluación de control interno, se comprobó que la Carrera Informática no cuenta con políticas, procedimientos o planes legalmente constituidos, que le permitan asegurar la continuidad de sus operaciones ante cualquier vulnerabilidad, basado en el establecimiento de medidas preventivas.
CRITERIO	Según la de Norma de Control Interno 410: La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria.
CAUSA	Las autoridades no han desarrollado las oportunas gestiones para dar cumplimiento en la documentación de las normativas vigentes respecto a la seguridad en la Carrera de Informática.
EFECTO	La ausencia de política de seguridad aprobada legalmente, evidencia el uso inadecuado de los recursos de tecnología de información por parte de los usuarios, exponiéndolos a riesgos que incluyen desde ataques de virus a los servicios y sistemas de redes, ingresos no autorizados a la red, hasta la sustracción de los equipos limitando inversiones futuras en mejora de los mismos, sometiéndolos a constantes peligros e incumplimiento de normativas legales.

CONCLUSIÓN
La aplicación de una política de seguridad documentada legalmente, proporcionará directrices a las autoridades en cuanto a la salvaguarda y prevención contra amenazas de los recursos tecnológicos y de la información disponible en la Carrera Informática, para proporcionar soporte significativo y relativo a la seguridad, de acuerdo a las leyes o normativas vigentes en el país, por lo que las autoridades deben asumir compromisos para aprobar y documentar los procedimientos.

RECOMENDACIONES PARA EL PROCESO DE MEJORA	**ESTAMENTO:**	**DIRECCIÓN DE CARRERA**
ELABORACIÓN DE NORMATIVA	***POLÍTICA DE SEGURIDAD EN LA CARRERA DE INFORMÁTICA***	
¿QUÉ PROTEGER?	Todos los recursos tecnológicos y la información física o electrónica que exista en la Carrera Informática, definiendo la ubicación, acceso, registro de mantenimiento preventivo o correctivo, fuera o dentro de la entidad.	
¿DE QUÉ?	De amenazas originadas por el ingreso no autorizado a la red usando contraseñas ajenas, ingreso a las áreas de personas no autorizadas o que no hayan sido registradas, robo, incendios, inundaciones, salida de información no autorizada.	
RESPONSABLES	Las personas que utilizan los recursos tecnológicos, directamente como el director, asistentes, secretaria, docentes, estudiantes de la Carrera Informática, entre otros. Indirectamente o terceras partes como, proveedores de servicios, docentes y estudiantes de otras coordinaciones, asumiendo todos roles y responsabilidades en la utilización del equipo en el uso exclusivo para propósitos legítimos de la entidad. Además los encargados de la asignación de autorización, y los custodios de llaves.	

DETECCIÓN DE HALLAZGOS		
ÁREA	**RESPONSABLE**	**ORIGEN**
Carrera Informática	**Director de Carrera**	**AUDITORÍA TECNOLÓGICA**

3 BASE LEGAL:	***Norma de Control Interno 410*** titulada ***Tecnología de la Información,*** referente a ***410-10 Seguridad de Tecnología de Información,*** y ***410-11 Plan de Contingencias.***
PROCEDIMIENTO	Comprobar la existencia de un Plan de Continuidad que proteja sus procedimientos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres.
CONDICIÓN	De acuerdo a la evaluación de control interno, se comprobó que la Carrera Informática no cuenta con políticas, procedimientos o planes legalmente constituidos, que le permitan asegurar la continuidad de sus operaciones ante cualquier vulnerabilidad, basado en el establecimiento de medidas preventivas.
CRITERIO	Según la de Norma de Control Interno 410: La máxima autoridad, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.
CAUSA	Las autoridades no han garantizado que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo bajo el cumplimiento de Normas de Control.
EFECTO	Al no contar con la implementación de planes para la continuidad de las operaciones, la Carrera Informática, puede ser víctima de posibles incidentes, una caída de la luz eléctrica, una inundación, un incendio o un robo han de considerarse amenazas reales que deben ser tratadas de forma preventiva para evitar, en caso de que éstas sucedan, que las pérdidas no sean tan graves y que afecten a la viabilidad de sus actividades.

CONCLUSIÓN
La Carrera Informática no cuenta con un Plan de Continuidad, que le permita seguir ante las posibles amenazas a las que está expuesta, lo que puede conllevar desde una pérdida importante de las prestaciones de servicios hasta un desastre natural, sin embargo, ante esta situación es imprescindible estar preparados con procedimientos, políticas y planes que mitiguen los riesgos. Por lo tanto, resulta necesario implementar un plan de continuidad del negocio que permita tener una respuesta efectiva a las interrupciones de las operaciones y cumplir con las disposiciones legales.

RECOMENDACIONES PARA EL PROCESO DE MEJORA	**ESTAMENTO:**	**DIRECCIÓN DE CARRERA**
ELABORACIÓN DE NORMATIVA	***PLAN DE CONTINUIDAD DE OPERACIONES EN LA CARRERA INFORMÁTICA***	
ASPECTO GENERAL	El plan establecerá, organizará y documentará los riesgos, responsabilidades, políticas, procedimientos y acuerdos, así mismo, proporcionará un enfoque organizado y consolidado para dirigir actividades de respuesta y recuperación ante cualquier incidente o interrupción de operaciones imprevista, evitando confusión y reduciendo la situación de tensión.	
LINEAMIENTOS	a) Creación de una política de continuidad de operaciones, b) Análisis del impacto, c) Estrategia de recuperación, c) Desarrollo del Plan de Continuidad de Operaciones, y d) Pruebas y mantenimiento.	

DETECCIÓN DE HALLAZGOS		
ÁREA	**RESPONSABLE**	**ORIGEN**
Carrera Informática	**Director de Carrera**	**AUDITORÍA TECNOLÓGICA**

4 BASE LEGAL:	***Norma de Control Interno 410*** titulada ***Tecnología de la Información,*** referente a ***410-10 Mantenimiento y control de la infraestructura tecnológica.***
PROCEDIMIENTO	Verificar si existen registros de mantenimiento a los recursos tecnológicos de la Carrera Informática.
CONDICIÓN	Conforme a la evaluación de control interno, se detectó que la Carrera Informática no cuenta registros documentados del mantenimiento de recursos tecnológicos.
CRITERIO	Según la de Norma de Control Interno 410: La unidad de tecnología de información de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades.
CAUSA	El departamento de Soporte Técnico brinda mantenimiento a los recursos tecnológicos de la ESPAM MFL en general, por ende no existen medidas establecidas que determinen las condiciones (Lugar, calendario, horario) en que debe llevarse el mantenimiento a los equipos y sistemas de la Carrera Informática, lo que genera inconvenientes a la hora de mejorar el desempeño y buen uso de los recursos tecnológicos.
EFECTO	En consecuencia el no contar con medidas establecidas para el mantenimiento de los recursos tecnológicos, estos se ven afectados, provocando fallos en su rendimiento.

CONCLUSIÓN
La Carrera Informática no cuenta con programas que garanticen el apropiado mantenimiento de sus recursos tecnológicos, razón por la cual estos son propensos a sufrir daños. Sin embargo, para el cumplimiento de los objetivos de la Carrera Informática, se requiere de una actividad programada de inspecciones, tanto de funcionamiento como de seguridad, ajustes, reparaciones, análisis, desempeño, que deben llevarse a cabo en forma periódica en base a un plan establecido. El propósito es prever averías o corregirlas para mantener las instalaciones, equipos y sistemas en niveles óptimos de operación.

RECOMENDACIONES PARA EL PROCESO DE MEJORA	**ESTAMENTO:**	**DIRECCIÓN DE CARRERA**
ELABORACIÓN DE NORMATIVA	***PLAN DE MANTENIMIENTO A LOS RECURSOS TECNOLÓGICOS EN LA CARRERA INFORMÁTICA***	
ASPECTO GENERAL	Realizar una planificación vinculada con el Departamento de Mantenimiento y Soporte Técnico de la ESPAM MFL, con la finalidad de mantener la infraestructura y equipos de la Carrera Informática en condiciones óptimas, y así cumplir con los objetivos institucionales.	
LINEAMIENTOS	• Establecer políticas orientadas a brindar mantenimiento a los recursos tecnológicos. • Elaborar inventarios actualizados de los recursos tecnológicos que posee la Carrera Informática, con la finalidad de facilitar las tareas de mantenimiento. • Determinar la necesidad de mantenimiento mediante la elaboración de una solicitud. • Elaborar un Programa de Mantenimiento con base a las lista de verificaciones, y atendiendo a las solicitudes recibidas. • Elaborar y presentar los informes periódicos de las actividades realizadas, con el propósito de obtener un registro de los recursos a los cuales se les proporciono mantenimiento y soporte técnico.	

ANEXO 10

SOLICITUD DE INFORMACIÓN

Solicitud de información con el Director de la Carrera Informática