ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

ESCUELA DE CONTABILIDAD Y AUDITORÍA

Carrera en Ingeniería en Contabilidad y Auditoría CPA.

TESIS DE GRADO

Previa a la obtención del Título de:

Ingeniero en Contabilidad y Auditoría C.P.A.

TEMA:

"AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN BAJO LAS NORMAS ISO/IEC 17799, EN LA RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO (REFICH). PERIODO 2012".

AUTORES:

MORALES GARCÉS JOSE LUÍS
VALLE ROMERO MARÍA LORENA

Riobamba – Ecuador

2014

CERTIFICACIÓN DEL TRIBUNAL

Certificamos que el presente trabajo de investigación sobre el tema "AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN BAJO LAS NORMAS ISO/IEC 17799, EN LA RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO (REFICH). PERIODO 2012" previo a la obtención del título de Ingeniero en Contabilidad y Auditoría C.P.A., ha sido desarrollado por el Srs. MORALES GARCÉS JOSE LUÍS y VALLE ROMERO MARÍA LORENA han cumplido con las normas de investigación científica y una vez analizado su contenido, se autoriza su presentación.

Ing. Mayra Alejandra Oñate Andino	Ing. Carlos Alfredo Ebla Olmedo
DIRECTOR DE LA TESIS	**MIEMBRO DEL TRIBUNAL**

CERTIFICADO DE RESPONSABILIDAD

Nosotros**,** MORALES GARCÉS JOSE LUÍS y VALLE ROMERO MARÍA LORENA, estudiante de la Escuela de Ingeniería en Contabilidad y Auditoría de la Facultad de Administración de Empresas, declaro que la tesis que presento es auténtica y original. Somos responsables de las ideas expuestas y los derechos de autoría corresponden a la Escuela Superior Politécnica de Chimborazo.

MORALES GARCÉS JOSE LUÍS

VALLE ROMERO MARÍA LORENA

DEDICATORIA

Han transcurrido varios años de constante estudio y sacrificio para alcanzar la ansiada meta, que no hubiese sido posible, sin el apoyo de mis padres Rubén y Maritza quienes fueron los promotores de que en el futuro sea un profesional útil para la sociedad; a mi hermano, amigos, familiares y maestros.

Y mi amada esposa quien es mi soporte en los momentos difíciles de mi existencia, y a la luz de mi corazón fruto de este amor las cuales me alientan para continuar y cumplir con mi objetivo propuesto que es la culminación de mi carrera profesional.

A ellos dedico este trabajo con mucho amor y cariño.

Jose Luis

Dedico este trabajo al arquitecto de la vida "Dios" porque está conmigo en cada paso que doy, guiándome, protegiéndome y dándome fortaleza para seguir adelante;

A mis padres Víctor y Fanny, por siempre darme el apoyo incondicional para mi educación y bienestar, a mis hermanos Víctor y Margarita por ser mi motivación en el transcurso de todo este tiempo, y a toda mi familia que me ayudo;

A mis amigas por ser tan buenas conmigo en momentos muy difíciles, por nunca dejarme sola, a esos amigos que nunca me dieron las espaldas y supieron brindarme sus sabios consejos;

Y a esas personas especiales en mi vida que me acompañaron en cada etapa fundamental de mi carrera para guiarme y darme fuerzas cada día para no rendirme en esos momentos de debilidad por haber estado allí cuando más los necesite;

A todos ustedes muchas gracias, los amo.

Ma. Lorena

AGRADECIMIENTO

Al culminar este trabajo es grato presentar nuestro reconocido agradecimiento, primeramente a Dios, a nuestra querida Escuela Superior Politécnica de Chimborazo, a la Escuela de Contabilidad y Auditoría por abrirnos las puertas del aprendizaje diario;

A todos los docentes quienes nos supieron guiar por el camino de la sabiduría, en especial a la Ing. Alejandra Oñate e Ing. Carlos Ebla quienes a lo largo de este tiempo nos orientaron con sus conocimientos en el desarrollo de nuestra tesis, la cual ha finalizado llenando todas nuestras expectativas;

A nuestros queridos padres por su apoyo incondicional en la culminación de nuestra carrera profesional;

Y finalmente agradecemos a la Red de Estructura de Finanzas Populares y Solidaria de Chimborazo por facilitarnos la información requerida para el desarrollo y culminación de nuestra tesis.

RESUMEN

En la presenta tesis se ha realizado una Auditoría Informática de la Seguridad de la Información bajo las normas ISO/IEC 17799, en la Red de Estructura de Finanzas Populares y Solidarias de Chimborazo, con la finalidad de evidenciar la vulnerabilidades existentes en la Seguridad de la Información en el Departamento de Control y Monitoreo de la entidad las mismas que se reflejaron después de hacer el análisis FODA y evaluando el nivel de control interno mediante los cuestionarios aplicados en cada uno de los parámetros que indica la norma ISO/IEC 17799, siendo estas las más destacadas Seguridad del Personal, Comunicación y Administración de Operaciones, Control de Accesos y la Continuidad del Negocio.

Los hallazgos que se determinaron fueron que la entidad no cuenta con acuerdos de confidencialidad en los contratos, que los respaldos de la información no se la realiza de manera oportuna, que es fácil el acceso a claves, y que no se ha considerado un plan para la mejora continua del negocio

Realizando las respectivas recomendaciones en el Informe de Auditoría dirigidas al Director Ejecutivo de la REFICH, las cuales aportaran para el mejoramiento de los procesos del manejo de la información en la entidad.

SUMMARY

In the presented thesis has been carried out an Audit of the Computing Security of the information under the rules ISO/IEC 17799, in the Network Structure of Popular and Solidarity Finances of Chimborazo, with the purpose of showing the existing vulnerabilities in the Security of the Information in Control and Monitoring Department of the same entity is reflected after doing the Strengths Weaknesses Opportunities and Threats (SWOT) analysis and evaluating the level of internal control through the questionnaires applied in each of the parameters indicating the standard ISO/IEC 17799, these being the most prominent of the Security Personnel, Communication and Operations Management, Access Control and Business Continuity.

The finding identified were that the entity does not have confidentiality agreements in contracts, which the seatbacks of the information is not done in a timely manner, which is easy access to key, and that has not been considered a plan to continuous improvement of business.

Performing the respective recommendations in the Audit Report to the Executive Director of the Network Structure of Popular and Solidarity Finances of Chimborazo, which contribute to the improvement of the processes of information management at the entity.

ÍNDICE DE CONTENIDOS

Título **Pág.**

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

INTRODUCCIÓN

La realización de la Auditoría Informática de la Seguridad de la Información bajo las normas ISO/IEC 17799 en la Red de Estructura De Finanzas Populares y Solidarias de Chimborazo se ha desarrollado en base al diagnóstico realizado a la entidad en la cual encontramos varios puntos vulnerables y áreas críticas.

El tipo de investigación utilizada es mixta por que se realiza en forma cualitativa ya que se tiene información directa de lo investigado por medio de la aplicación de una entrevista; y de forma cuantitativa porque podemos determinar cuántos hallazgos hemos encontrado en la auditoría.

El primer capítulo está comprendido por problematización, objetivos propuestos para el cumplimiento de la investigación. El segundo capítulo se presenta las referencias teóricas como el Hilo Conductor, Antecedentes Investigativos, Definición de Auditoría, Auditoría Informática, Seguridad de la información y descripción de la Norma ISO/IEC 17799. El tercer capítulo está representado por el Marco Metodológico que consta de la Idea a Defender, Tipos de Investigación, Métodos Técnicas e Instrumentos y la verificación de la Idea a Defender. El cuarto capítulo se encuentra una guía para aplicar la Auditoría Informática para la Seguridad de la Información en la cual se aplicó las cuatro fases de la Auditoría (Diagnostico General, Planificación, Ejecución y Comunicación) para el desarrollo de la investigación

Finalmente se muestra las conclusiones y recomendaciones obtenidas del proceso investigativo, dirigidas al Director Ejecutivo tomando la mejor decisión para la entidad en los procesos del manejo de la información de la Red de Estructura de Finanzas Populares y Solidarias de Chimborazo.

CAPÍTULO I

1. PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Al pasar el tiempo muchas empresas u organizaciones, se han enfrentado y han logrado integrarse a nuevos avances tecnológicos, los cuales son el resultado de muchos esfuerzos, dedicación y trabajo continuo de innumerables profesionales.

La Ley de Economía Popular y Solidaria y su Reglamento, exige que toda institución financiera deba entregar información oportuna en plazo y características. Mandatos y disposiciones que alarma a directivos, empleados y administradores. Así también el mercado competitivo exige que productos y servicios estén técnicamente diseñados para lograr un crecimiento sostenido.

La Red de Estructura de Finanzas Populares y Solidarias de Chimborazo, tiene el propósito de cumplir con las regulaciones y exigencias normativas, fortalecer su estructura organizacional y administrativa que le permita generar ventajas competitivas que le aseguren la sostenibilidad y sustentabilidad en el sistema económico popular, con la finalidad de ampliar sus productos y servicios a más sectores de la provincia de Chimborazo.

La Red de Estructura de Finanzas Populares y Solidarias de Chimborazo (REFICH) al no evaluar su sistema de protección de la información y comunicación informática, se encuentra expuesta a los riesgos organizacionales, operacionales y físicos de la entidad, causando pérdidas económicas y afectando su imagen corporativa.

1.1.1 Formulación del problema de investigación

No existe un modelo de evaluación para el sistema de información, que facilite la identificación de puntos vulnerables y errores que mejoren las operaciones en el Departamento de Control y Monitoreo en la Red de Estructura de Finanzas Populares y Solidarias de Chimborazo (REFICH).

1.1.2 Delimitación del Problema

El objeto de esta investigación es la Auditoría y su campo se enmarca en la Auditoría Informática de la Seguridad de la Información bajo las normas ISO/IEC 17799, la cual se desarrollará en la Red de Estructura de Finanzas Populares y Solidarias de Chimborazo.

1.2 OBJETIVOS

1.1.3 Objetivo General

Desarrollar una Auditoría Informática de la seguridad de la información basada en la norma ISO/IEC 17799 con la finalidad de plantear las medidas y controles que mejoren las operaciones de la Unidad Gestión de Sistemas y Monitoreo en la Red de Estructura de Finanzas Populares y Solidarias de Chimborazo (REFICH). Periodo 2012.

1.1.4 Objetivos Específicos

- Realizar un análisis bibliográfico documental respecto a la Auditoría Informática, Sistema de Información y la norma ISO/IEC 17799 como elementos que direccionen la investigación.

- Evaluar el Sistema de Información en la Red de Estructura de Finanzas Populares y Solidarias de Chimborazo aplicando la norma ISO/IEC 17799.

- Emitir informe de auditoría con recomendaciones para el mejoramiento del Departamento de Control y Monitoreo.

1.3 JUSTIFICACIÓN DEL PROBLEMA

La finalidad de Auditoría Informática de la Seguridad de la Información bajo las normas ISO/IEC 17799 es de determinar el informe del trabajo realizado para tomar las medidas correctivas pertinentes a cada uno de los casos encontrados con el propósito de proteger la información de La Red de Estructura de Finanzas Populares y Solidarias de Chimborazo.

Los activos de información son recursos que representan una gran importancia y costos vitales para la Red de Estructura de Finanzas Populares y Solidarias de Chimborazo. Si

estos activos llegaran a fallar la Red quedaría en una situación ineficiente en la continuidad de los procesos de las pequeñas cajas y bancos comunales que están vinculados, y por tal razón la Red de Estructura de Finanzas Populares y Solidarias de Chimborazo, deberán salvaguardar la información. Esto implica tomar las acciones apropiadas sobre la seguridad de la información las mismas que deben ser basadas en la protección de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorción, violación de la privacidad, intrusos, hackers interrupción de servicio, accidentes y desastres naturales que todos los activos están expuestos.

El presente proyecto ayudara en la aplicación de las normas ISO/IEC 17799 contribuyendo así a los conocimientos ya obtenidos en la cátedra de Auditoría Informática, siendo esta investigación en una fuente de consulta.

CAPÍTULO II

2. MARCO TEÓRICO

2.1 HILO CONDUCTOR

Mediante el hilo conductor elaboramos el marco teórico, en donde mencionaremos temas como antecedentes investigativos, auditoría, auditoría informática, seguridad de la información, y sobre las normas emitidas por la ISO/IEC 17799 en cuanto se refiera a la seguridad de la información que nos sirve como fundamento teórico para la realización de este trabajo.

GRÁFICO N° 1 Hilo Conductor.

Fuente: Auditoría Informática
Elaborado por: Jose L. Morales & Ma. Lorena Valle.

2.2 ANTECEDENTES INVESTIGATIVOS

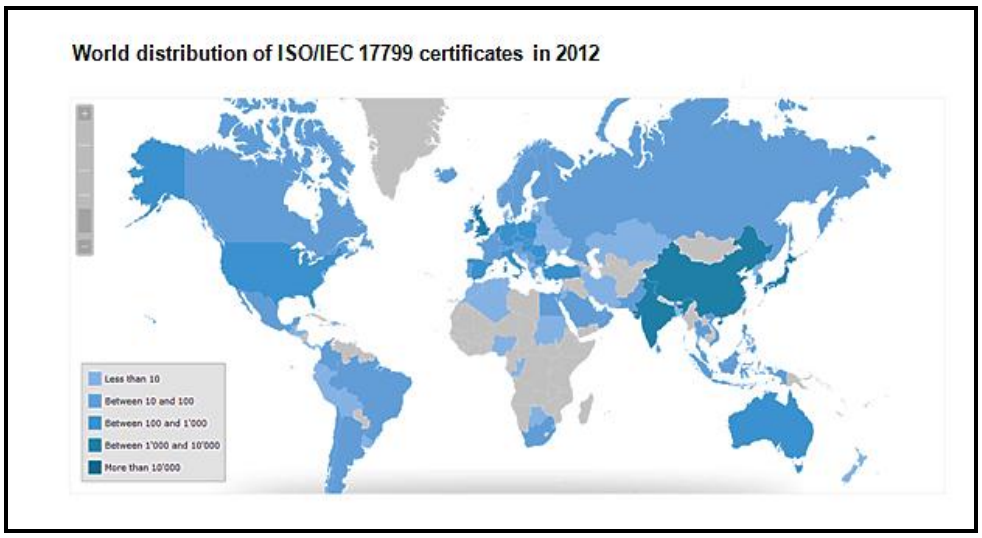
Según la compilación bibliográfica de Castro J. (2010) nos indica que desde a inicio del siglo XIX en el año 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution) es responsable de la publicación de importantes normas como:

- 1979 Publicación BS 5750 – ahora ISO 9001
- 1992 Publicación BS 7750 – ahora ISO 14001
- 1996 Publicación BS 8800 – ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa británica un conjunto de buenas prácticas para la gestión de la seguridad de su información. La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un Sistema Gestión de Seguridad de la Información (SGSI) para ser certificable por una entidad independiente. Las dos partes de la normas BS 7799 se revisaron en 1999 y la primera parte se adoptó por International Organization for Standardization (ISO), sin cambios sustanciales, como ISO 17799 en el año 2000. Tras un periodo de revisión y actualización de los contenidos del estándar se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005, en España existe la publicación nacional UNE-ISO/IEC 17799 que fue elaborada por el comité técnico AEN/CTN 71 y titulada Código de buenas prácticas para la Gestión de la Seguridad de la Información que es una copia idéntica y traducida del Inglés de la Norma Internacional ISO/IEC 17799:2000, la edición en español equivalente a la revisión ISO/IEC 17799:2005.

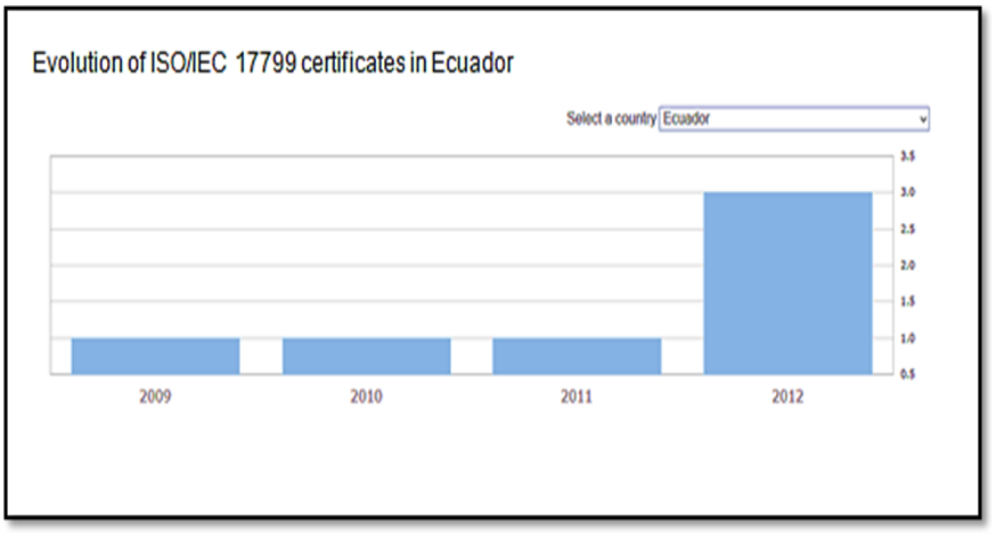
Esta norma es utilizada a nivel mundial por 70 países los cuales adoptado la norma ISO 17799 (THE ISO SURVEY, 2012). Según la página WEB de Certificaciones ISO 17799, Japón encabeza los países con el mayor número de certificaciones del SGSI, seguida por la India y Reino Unido. En Latinoamérica: México, Brasil, Colombia, Perú, Argentina y Ecuador con 3 certificaciones, es un nivel inferior en la comparación mundial.

GRÁFICO N° 2 Distribución de certificaciones a nivel mundial en el 2012.



Fuente: The ISO Survey, 2012.

GRÁFICO N° 3 Evolución de la ISO/IEC 17799 en Ecuador en el año 2012.



Fuente: The ISO Survey, 2012.

A nivel mundial hay leyes que protegen la Seguridad de la Información en según la (OMB, 2008) en Norteamérica la Ley Federal de Gestión de Seguridad de la Información (FISMA, 2002) habiendo logrado un cumplimiento más del 93% en materia de Seguridad de Información; en tanto en Europa nos indica (ASIMELEC, 2003) que el gobierno de Reino Unido se recomendó como parte de su Ley de Protección a la Información en la cual indica que las compañías británicas utilicen BS 7799, también nos señala que el fundamento en la norma ISO desarrollada por un comité internacional y multidisciplinar de expertos, para que una organización tenga un

buen nivel de seguridad debería tener plenamente implementada el 90% de las recomendaciones de la norma ISO 17799; el nivel de implementación en España de esta norma es del 53%, teniendo como mayor obstáculo a la implementación de esta norma es la cultura empresarial, por encima de los problemas previos que podrían parecer más relevantes como presupuesto o tecnología.

Otro estudio Internacionalmente importante revisado es una investigación titulada "Critical success factors and requirements for achieving business benefits from in formation security" (Partida, Ezingerad, 2007). Realizado en Henley Management College de Reino Unido por Alberto Partida y Jean-Noël Ezingeard. En el mencionado estudio, a través de una encuesta a más de 80 profesionales de la Seguridad de la Información y expertos a nivel mundial se muestra que las organizaciones que desarrollan prácticas de Seguridad de la Información en base a un fuerte compromiso de la alta dirección, integrando sus procesos de administración de riesgos incluyendo la Seguridad de la Información alineados a los objetivos estratégicos, obtienen beneficios superiores. En este mismo estudio, se señala que los tres beneficios más comunes son:

- Valor incremental para los accionistas.
- Nuevas oportunidades de negocios.
- Mejor gobierno (cumplimiento).

Según la Encuesta Nacional sobre Seguridad Informática realiza en México por (UNIVA, 2008), en los cuales sus resultados fueron que la norma de la seguridad ISO/IEC 17799 no supera ni el 50% de implementación en la Seguridad de la Información por algunos factores como la inexistencia de política de seguridad, falta de tiempo, formación técnica, capacitación y apoyo directivo. También se puede apreciar que la adopción de la norma internacional está progresando sostenidamente a nivel mundial y regional principalmente en Europa, Asia y América del Norte, (Ernst &Young's, 2006), donde se destaca España, Reino Unido, Japón y Estados Unidos, en Latino América se destaca Brasil, Colombia y Chile, informaciones recogidas utilizando como herramienta principal las encuestas (The ISO Survey, 2012), asimismo señalar que la estandarización de la norma también va acompañado por el desarrollo de las capacidades humanas especializadas cuya formación y certificación es administrada por

importantes organismos independientes reconocidos Internacionalmente. A continuación presentamos los trabajos destacados de la región:

"Aplicación de la Norma ISO/IEC 17799 en las Empresas de la Región del Maule" elaborado por Clorindo Antonio Fuenzalida de la Parra trabajo realizado en Santiago de Chile- Chile en el 2005 en cuyas conclusiones dice lo siguiente:

Los resultados obtenidos plantean que no existe un nivel de discordancia la que permita establecer categóricamente que tanto encargados informáticos de la empresas como auditores con experiencia, den un nivel distinto de riesgo a las medidas de riesgo de la ISO 17799, así como también que los encargados entreguen un mayor nivel de riesgo que los auditores a dichas medidas planteadas en la norma, ya que existen muchos puntos en que estos tipos concuerdan o difieren desde el planteamiento del auditor.

"Factores inhibidores en la Implementación de Sistemas de Gestión de la Seguridad de la Información basado en la NTP- ISO/IEC 17799 en la administración pública." elaborado por Alipio Mariño Obregón trabajo realizado en Lima- Perú en el 2010 en la cual concluyó lo siguiente:

No hay, un entendimiento claro sobre la responsabilidad global de la seguridad de la información dentro de la institución, lo cual se refleja en que el nivel de liderazgo para la implementación mayormente descansa en los gerentes o jefes de área de informática y sin el compromiso de la alta dirección, con un enfoque de seguridad informática más que a la seguridad de la información. Por las razones expuestas, esta investigación, ha determinado que el bajo nivel alcanzado en la implementación de la Norma de Seguridad en los Organismos Públicos Descentralizados Adscritos a la Presidencia del Consejo de Ministros (PCM) tiene como causa principal el hecho de que la Seguridad de la Información a pesar de formar parte de los objetivos estratégicos.

"Plan de Implementación de un Sistema de Seguridad de la Información, bajo la norma ISO 17799:2005 en Andinatel s.a." elaborado por Mercedes Torres Bueno trabajo realizado en Quito- Ecuador en el 2007 la cual concluye a continuación:

El plan desarrollado en esta tesis fue conocida y evaluada por los directivos de Andinatel S.A., Vicepresidenta de Sistemas, Gerente de control informático, quienes a través de documentos adjuntos, indican que se está ejecutando este plan de

implementación de seguridad de la información y además se lo remite a Contraloría Interna, en cumplimiento a sus recomendaciones indicando que la aplicación de la norma ISO 17799:2005 es eficaz para el control de la información dentro de la institución, se encuentra apoyada por la tecnología informática quienes manejan los medios de transmisión de la información interna de la empresa, el área técnica de operaciones y comunicaciones son núcleo del desarrollo del producto del negocio, cuenta también con el apoyo de la otra parte funcional, encontrándose las áreas administrativa, financiera y comercial, a estas también apoya el área informática de Andinatel para la gestión y procedimientos de la información.

En el Ecuador, las iniciativas sobre la adopción de la norma de seguridad de la información trata de seguir la tendencia internacional y se alinea con objetivos estratégicos que marca el frente para las estrategias de desarrollo de la sociedad de la Información, las cuales se han implementado con éxito el uso y buenas prácticas de este modelo y se cuenta actualmente con profesionales certificados en Auditoría, Analistas de Riesgos y Calidad de Procesos, por lo cual nos hemos basados en estos antecedentes para desarrollar nuestra investigación.

2.3 AUDITORÍA

2.3.1 Definición de Auditoría

La auditoría se la puede definir de diferentes puntos de utilización y práctica que se tienda a utilizar es así que tenemos algunas definiciones de autores especializados en la materia:

Porter W. & Burton J. (1983) Define la Auditoría como el examen de la información por una tercera persona distinta de quien la preparó y del usuario, con la intención de establecer su veracidad; y el dar a conocer los resultados de este examen, con la finalidad de aumentar la utilidad de tal información para el usuario.

Holmes A. (1984) obtiene como conclusión en su concepto moderno que la Auditoría es el examen crítico y sistemático de la actuación y los documentos financieros y jurídicos en que se refleja, con la finalidad de averiguar la exactitud, integridad y autenticidad de los mismos.

Sánchez C. (2006) la define así La Auditoría es el examen integral sobre la estructura, las transacciones y el desempeño de una entidad económica, para contribuir a la oportuna prevención de riesgos, la productividad en la utilización de los recursos y el acatamiento permanente de los mecanismos de control implantados por la administración.

Mientras que el Instituto Norteamericano de Contadores Públicos (AICPA, 1983), tiene como definición de Auditoría la siguiente:

Un examen que pretende servir de base para expresar una opinión sobre la razonabilidad, consistencia y apego a los principios de contabilidad generalmente aceptados, de estados financieros preparados por una empresa o por otra entidad para su presentación al público o a otras partes interesadas.

La anterior definición aunque es de las más favorecidas, puede ser considerada como muy sectorizada, pues no comprende en manera alguna toda la gama de auditorías existentes y las que se desarrollaran en el futuro y se queda limitada solamente a la Auditoría de los estados financieros.

La American Accounting Asociación (AAS, 1972) con un criterio más amplio y moderno define en forma general la Auditoría identificándola como un proceso de la siguiente manera. "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".El fin del proceso consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como determinar si dichos informes se han elaborado observando principios establecidos para el caso.

Utilizando las anteriores definiciones, la Auditoría puede conceptualizarse entonces como:

El proceso que consiste en el examen crítico, sistemático y representativo del sistema de información de una empresa o parte de ella, realizado con independencia y utilizando técnicas determinadas, con el propósito de emitir una opinión profesional sobre la misma, que permitan la adecuada toma de decisiones y brindar recomendaciones que mejoren el sistema examinado.

2.4 AUDITORÍA INFORMÁTICA

2.4.1. Definición de Auditoría Informática

Según Muñoz Razo Carlos (2002), la Auditoría Informática al igual que el resto de auditorías también tiene sus antecedentes, radicado en las publicaciones de los siguientes autores:

Echenique (1988), publicó su libro A*uditoría de Sistemas*, en el cual establece sus principales bases para el desarrollo de una auditoría de sistemas computacionales, dando un enfoque teórico práctico sobre el tema.

Hernández (1996), propone la Auditoría en Informática, en la cual da ciertos aspectos relacionados con esta disciplina.

Ávila (1997), obtiene mención honorifica en su examen profesional, en la Universidad de Valle de México, Campus San Rafael, con una tesis en la cual propone un caso práctico de la auditoría de sistemas realizado en una empresa estatal.

Yann (1998), presenta T*écnicas de auditoría*, donde hace una propuesta de diversas herramientas de esta disciplina.

Piattini & Del Peso (1998), presentan *Auditoría Informática*, un *enfoque práctico*, donde mencionan diversos enfoques y aplicaciones de esta disciplina.

Esta es la definición de Weber R. (1982), sobre auditoría informática en la cual indica que es una función que ha sido desarrollada para asegurar la salvaguarda de los activos de los sistemas de computadoras, mantener la integridad de los datos y lograr los objetivos de la organización en forma eficaz y eficiente.

Mientras que Mair W. (1987), define lo siguiente: La auditoría informática es la revisión y evaluación de los controles, sistemas y procedimientos de la informática; 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, confiable y segura de la información que servirá para una adecuada toma de decisiones.

Muñoz R (2002), define a la Auditoría Informática como la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e

información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumos necesarios para el funcionamiento del centro de cómputo. El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas informáticos a la empresa.

Es el conjunto de actividades realizadas por profesionales del área de auditoría e informática; dirigidos a la verificación y aseguramiento para que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología informática en la organización se realiza de manera oportuna y eficiente.

2.4.2 Objetivos de la Auditoría Informática

Según Poveda J. (2012) describe los siguientes objetivos de la auditoria informática como:

- Mejorar la Situación de la Empresa.
- Sugerir mejoras en controles, procedimientos, etcétera.
- Detectar fallas.
- Reunir elementos para la toma de decisiones.
- Reducir los riegos.
- Retroalimentar oportunamente.
- Optimizar el uso de recursos.
- Analizar imparcialmente las funciones.

Pero Vargas J. (2009) también nos dice que los objetivos de auditoría informática son:

- Verificar el control interno de la función informática.

- Asegurar a la alta dirección y al resto de las áreas de la empresa que la información que les llega es la necesaria en el momento oportuno, y es fiable, ya que les sirve de base para tomar decisiones importantes.

- Eliminar o reducir al máximo la posibilidad de pérdida de la información por fallos en los equipos, en los procesos o por una gestión inadecuada de los archivos de datos.

- Detectar y prevenir fraudes por manipulación de la información o por acceso de personas no autorizadas a transacciones que exigen trasvases de fondos.

Entonces podemos indicar que los objetivos de la auditoria informática son los siguientes: es el control de la función informática, el análisis de la eficiencia de los sistemas informáticos, la revisión de la eficaz gestión de los recursos informáticos, detección de fraudes por el mal manejo de la información, prevención de la manipulación de la información por personas no autorizadas.

2.4.3 Importancia de la Auditoría Informática

Según Hernández (1996), nos indica que siempre ha existido la preocupación por parte de las organizaciones por optimizar todos los recursos con que cuenta la entidad, sin embargo por lo que respecta a la tecnología de informática, es decir, software, hardware, sistemas de información, investigación tecnológica, redes locales, bases de datos, ingeniería de software, telecomunicaciones, etc. esta representa una herramienta estratégica que representa rentabilidad y ventaja competitiva frente a sus similares en el mercado, en el ámbito de los sistemas de información y tecnología un alto porcentaje de las empresas tiene problemas en el manejo y control, tanto de los datos como de los elementos que almacena, procesa y distribuye.

Vargas (2009), nos indica que la información es la parte fundamental de toda empresa para tener un alto nivel de competitividad y posibilidades de desarrollo. En la asamblea organizada por la compañía Bayer titulada Science for a better life, (La ciencia para una

mejor vida) celebrada en Centroamérica y El Caribe acentuaron cómo tema de discusión la Privacidad de la Información en las empresas y entidades indicando cual importante es conocer el significado de la función informática, de forma esencial cuando su manejo está basado en tecnología actual, para esto se debe conocer que la información: Esta almacenada y procesada en computadoras. Puede ser confidencial para algunas personas o a escala institucional. Puede ser mal utilizada o divulgada. Puede estar sujeta a robos, sabotaje o fraudes. El propósito de la revisión de la auditoria informática, es el de verificar que los recursos, es decir, información, energía, dinero, equipo, personal, programas de cómputo y materiales son adecuadamente coordinados y vigilados por la gerencia o por quien ellos designen.

2.4.4 Tipos de Auditoría Informática

Según Hernández E. (1996) y Vargas J. (2009) concuerdan en los tipos auditoría informática destacándolos siguientes posibles tipos:

- Auditoría de la gestión: referido a la contratación de bienes y servicios, documentación de los programas, etc.

- Auditoría legal del Reglamento de Protección de Datos: cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.

- Auditoría de los datos: clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.

- Auditoría de las bases de datos: controles de acceso, de actualización, de integridad y calidad de los datos.

- Auditoría de la seguridad: referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.

- Auditoría de la seguridad física: referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta.

- Auditoría de la seguridad lógica: comprende los métodos de autenticación de los sistemas de información.

- Auditoría de las comunicaciones: se refiere a la auditoria de los procesos de autenticación en los sistemas de comunicación.

- Auditoría de la seguridad en producción: frente a errores, accidentes y fraudes producidos en la producción.

Es por esto que en la actualidad, la Auditoria Informática es parte integral de las empresas, para ofrecer productos y servicios de alta calidad que se ajusten a las necesidades y preferencias del mercado, donde la información y la tecnología que la soporta, representan los activos más valiosos de la entidad, reconociendo así los beneficios potenciales que esta puede proporcionar para el éxito y la supervivencia de las mismas.

2.5 SEGURIDAD DE LA INFORMACIÓN

2.5.1. Definición Seguridad de la Información

Según Villalón A. (2004) nos indica que la seguridad de la información se define como la preservación de:

- **Confidencialidad**. Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.

- **Integridad.** Garantía de la exactitud y competencia de la información y de los métodos de su procesamiento.

- **Disponibilidad**. Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Vethius (2008), nos indica que la Seguridad de la Información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware, por lo que se necesita establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos.

Según Castro J. (2010), la Seguridad de la Información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. El concepto de Seguridad de la Información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

Para el hombre como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo. El campo de la Seguridad de la Información ha crecido y evolucionado considerablemente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial. Este campo ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, planificación de la continuidad del negocio, ciencia forense digital y administración de sistemas de gestión de seguridad, entre otros.

Conceptualizamos a la seguridad de la información como el aseguramiento de la confidencialidad, integridad y disponibilidad mediante controles en los que se incluyen varios procesos como la implementación de políticas y procedimientos los mismos que deberán ser implementados, controlados y mejorados cuando sean necesarios y lograr cumplir con el correcto manejo de la seguridad de la información.

2.5.2. Familia ISO Seguridad de la Información

GRÁFICO N° 4 Evolución Histórica de la ISO.

Fuente: Villalón A. 2004

Según Castro J. (2010), la BSI (British Standards Institution), la organización británica equivalente a AENOR (Asociación Española de Normalización y Certificación) en España es responsable de la publicación de importantes normas como: 1979 Publicación BS 5750 ahora ISO 9001, 1992 Publicación BS 7750 ahora ISO 14001, 1996 Publicación BS 8800 ahora OHSAS 18001. La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa, británica o no, un conjunto de buenas prácticas para la gestión de la seguridad de su información. La primera parte de la norma (BS 77991) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un SGSI (Sistema de Gestión de la Seguridad de la Información) para ser certificable por una entidad independiente. Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión. En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio del 2007, manteniendo el contenido así como el año de publicación formal de la revisión. En Marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

Según Humphrey T. (2005), la versión revisada de este estándar provee a las organizaciones de muchas mejoras e información sobre las mejores prácticas en seguridad de la información. Por ejemplo, mejores acuerdos de gestión de seguridad con agentes externos y proveedores de servicio, problemas de gestión de parches, dispositivos móviles, tecnologías inalámbricas y códigos dañinos vía Internet, mejoras en mejores prácticas en administración de recursos humanos y otras nuevas características.

2.5.3. Normas ISO/IEC 17799

Según Villalón A. (2004) Considerando las amenazas, cada vez más sofisticadas y en aumento, a las cuales está expuesta la información de las organizaciones, indica que surge la necesidad de definir pautas para resguardarla. En el Código de Práctica para la Gestión de la Seguridad de la Información, poco conocida por la profesión contable.

Esta representa un estándar reconocido internacionalmente, considerando que las empresas de todo tamaño o naturaleza tienen, en menor o mayor medida, un cierto nivel de dependencia informática, lo que implica que sean más vulnerables a los retos de seguridad.Surgida de la norma británica BS 7799, la norma ISO 17799 ofrece instrucciones y recomendaciones para la administración de la seguridad. La norma 17799 también ofrece una estructura para identificar e implementar soluciones para los siguientes riesgos:

- ***Política de Seguridad:*** escribir y comunicar la política de seguridad de la compañía.

- ***Organización de Seguridad***: definir los roles y las responsabilidades. Monitorear a los socios y a las empresas.

- ***Clasificación y Control de Activos:*** llevar un inventario de los bienes de la compañía y definir cuán críticos son así como sus riesgos asociados.

- ***Seguridad del Personal:*** contratación, capacitación y aumento de concientización relacionadas a la seguridad.

- ***Seguridad Física y del Entorno:*** área de seguridad, inventarios del equipamiento de seguridad.

- ***Comunicación / Administración de Operaciones:*** procedimientos en caso de accidente, plan de recuperación, definición de niveles de servicio y tiempo de recuperación, protección contra programas ilegales, etc.

- ***Control de Acceso:*** establecimiento de controles de acceso a diferentes niveles (sistemas, redes, edificios, etc.).

- ***Desarrollo y mantenimiento del sistema:*** consideración de la seguridad en sistemas desde el diseño hasta el mantenimiento.

- ***Plan de continuidad empresarial:*** definición de necesidades en términos de disponibilidad, recuperación de tiempo y establecimiento de ejercicios de emergencia.

- ***Cumplimiento Legal:*** respeto por la propiedad intelectual, las leyes y las reglamentaciones de la compañía.

Según Castro J. (2010), en toda organización que haga uso de las tecnologías de información se recomienda implementar buenas prácticas de seguridad, pues en muchas ocasiones el no seguir un proceso de implementación adecuado como el que establece el ISO 17799 puede generar huecos por la misma complejidad de las organizaciones, en ese sentido, aumenta la posibilidad de riesgos en la información. Este estándar internacional de alto nivel para la administración de la seguridad de la información, fue publicado por la ISO (International Organization for Standardization) en diciembre de 2000 con el objeto de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones. El ISO 17799, al definirse como una guía en la implementación del sistema de administración de la seguridad de la información, se orienta a preservar los siguientes principios de la seguridad informática:

- Confidencialidad.
- Integridad.
- Disponibilidad.

El objetivo de la seguridad de los datos es asegurar la continuidad de las operaciones de la organización, reducir al mínimo los daños causados por una contingencia, así como optimizar la inversión en tecnologías de seguridad. Como todo buen estándar, el ISO 17799 da la pauta en la definición sobre cuáles metodologías, normas o estándares técnicos pueden ser aplicados en el sistema de administración de la seguridad de la información, se puede entender que estos estándares son auxiliares y serán aplicados en algún momento al implementar el mismo. Hemos determinado que aplicación de un marco de referencia de seguridad basado en el ISO 17799 proporciona beneficios a toda organización que lo implemente, al garantizar la existencia de una serie de procesos que permiten evaluar, mantener y administrar la seguridad de la información.

Según Cervantes (2011), la norma ISO/IEC 17799 también ofrece una estructura para identificar e implementar soluciones para los siguientes riesgos:

- ***Política de Seguridad:*** escribir y comunicar la política de seguridad de la compañía.

TABLA N° 1: POLÍTICA DE SEGURIDAD

Objetivo	Proporcionar la guía y apoyo de la Dirección para la Seguridad de la Información en relación a los requisitos del negocio y a las leyes y regulaciones relevantes.
Principios	La Dirección debe establecer una política clara y en línea con los objetivos del negocio y demostrar su apoyo y compromiso con la Seguridad de la Información mediante la publicación y mantenimiento de una política de seguridad de la información para toda la organización.
Métrica	Cobertura de la política (es decir, porcentaje de secciones de ISO/IEC 17799 para las cuales se han especificado, escrito, aprobado y publicado políticas y sus normas, procedimientos y directrices asociadas. Grado de despliegue y adopción de la política en la organización (medido por auditoría, gerencia o autoevaluación).

Fuente: Cervantes.
Elaborado por: Ma. Lorena Valle & Jose L. Morales

- ***Organización de Seguridad:*** definir los roles y las responsabilidades. Monitorear a los socios y a las empresas.

TABLA N° 2 ORGANIZACIÓN DE SEGURIDAD

Objetivo	Gestionar la Seguridad de la Información dentro de la Organización tanto interna como externa.
Principios	Establecer una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro de la Organización. El órgano de dirección debe aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implantación de la seguridad en toda la Organización. Si fuera necesario, en la Organización se debería establecer y facilitar el acceso a una fuente especializada de consulta en seguridad de la información. Deberían desarrollarse contactos con especialistas externos en seguridad, que incluyan a las administraciones pertinentes, con

	objeto de mantenerse actualizado en las tendencias de la industria, la evolución de las normas y los métodos de evaluación, así como proporcionar enlaces adecuados para el tratamiento de las incidencias de seguridad. Control de acceso de terceros a los dispositivos de tratamiento de información de la organización. Cuando el negocio requiera dicho acceso de terceros, se debe realizar una evaluación del riesgo para determinar sus implicaciones sobre la seguridad y las medidas de control que requieren. Estas medidas de control deberían definirse y aceptarse en un contrato con la tercera parte.
Métrica	Porcentaje de funciones/unidades organizativas para las cuales se ha implantado una estrategia global para mantener los riesgos de seguridad de la información por debajo de umbrales explícitamente aceptados por la dirección. Porcentaje de empleados que han (a) recibido y (b) aceptado formalmente, roles y responsabilidades de seguridad de la información. Porcentaje de conexiones con terceras partes que han sido identificadas, evaluadas en cuanto a su riesgo y estimadas como seguras.

Fuente: Cervantes
Elaborado por: Ma. Lorena Valle & Jose L. Morales

- **Clasificación y Control de Activos:** llevar un inventario de los bienes de la compañía y definir cuán críticos son así como sus riesgos asociados.

TABLA N° 3 CLASIFICACIÓN Y CONTROL DE ACTIVOS

Objetivo	Alcanzar y mantener una protección adecuada de los activos de la Organización y asegurar que se aplica un nivel de protección adecuado a la información (clasificación).
Principios	Todos los activos deben ser justificados y tener asignado un propietario. Identificar a los propietarios para todos los activos y asignarles la responsabilidad del mantenimiento de los controles adecuados. La implantación de controles específicos podría ser delegada por el propietario convenientemente. Se debe clasificar la información para indicar la necesidad, prioridades y nivel de protección previsto para su tratamiento. Debe utilizarse un esquema de clasificación de la información para definir el

	conjunto adecuado de niveles de protección y comunicar la necesidad de medidas especiales para el tratamiento.
Métrica	Porcentaje de activos de información en cada fase del proceso de clasificación (identificado / inventariado / propietario asignado / riesgo evaluado / clasificado / asegurado). Porcentaje de activos de información claves para los cuales se ha implantado una estrategia global para mitigar riesgos de seguridad de la información según sea necesario y para mantener dichos riesgos en niveles aceptables. Porcentaje de activos de información en cada categoría de clasificación (incluida la de "aun sin clasificar").

Fuente: Cervantes
Elaborado por: Ma. Lorena Valle & Jose L. Morales

- **Seguridad del Personal:** contratación, capacitación y aumento de concientización relacionadas a la seguridad.

TABLA N° 4 SEGURIDAD DEL PERSONAL

Objetivo	Asegurar que los empleados, contratistas y usuarios de terceras partes entiendan: Sus responsabilidades y sean aptos para las funciones que desarrollen. Se encuentren equipados para cumplir con la política de seguridad de la organización en el desempeño de sus labores diarias, para reducir el riesgo asociado a los errores humanos. Entiendan la política para el abandono de la organización o cambio de empleo en forma organizada. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.
Principios	Definir responsabilidades de la Dirección para garantizar que la seguridad se aplica en todos los puestos de trabajo de las personas de la organización. Las responsabilidades de la seguridad se deberían definir antes de la contratación laboral mediante la descripción adecuada del trabajo y los términos y condiciones del empleo. Todos los candidatos para el empleo, los contratistas y los usuarios de terceras partes deben ser seleccionados adecuadamente, especialmente para los trabajos sensibles. Los empleados, contratistas y usuarios de terceras partes de los servicios de procesamiento de la información deben firmar un acuerdo sobre sus funciones y responsabilidades con

	relación a la seguridad. A todos los usuarios empleados, contratistas y terceras personas se les debería proporcionar un adecuado nivel de concienciación, educación y capacitación en procedimientos de seguridad y en el uso correcto de los medios disponibles para el procesamiento de la información con objeto de minimizar los posibles riesgos de seguridad. Se deberían establecer las responsabilidades para asegurar que el abandono de la organización por parte de los empleados, contratistas o terceras personas se controla, que se devuelve todo el equipamiento y se eliminan completamente todos los derechos de acceso.
Métrica	Porcentaje de nuevos empleados o pseudo-empleados (contratistas, consultores, temporales, etc.) que hayan sido totalmente verificados y aprobados de acuerdo con las políticas de la empresa antes de comenzar a trabajar. Respuesta a las actividades de concienciación en seguridad. Porcentaje de identificadores de usuario pertenecientes a personas que han dejado la organización, separados por las categorías de activos (pendientes de desactivación) e inactivos (pendientes de archivo y borrado).

Fuente: Cervantes
Elaborado por: Ma. Lorena Valle & Jose L. Morales

- **Seguridad Física y del Entorno:** área de seguridad, inventarios del equipamiento de seguridad**.**

TABLA N° 5 SEGURIDAD FÍSICA Y DEL ENTORNO

Objetivo	Evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de la organización (áreas seguras). Evitar la pérdida, daño, robo o puesta en peligro de los activos e interrupción de las actividades de la organización (seguridad de equipos).
Principios	Los servicios de procesamiento de información sensible deben ubicarse en áreas seguras y protegidas en un perímetro de seguridad definido por barreras y controles de entrada adecuados. Estas áreas deberían estar protegidas físicamente contra accesos

	no autorizados, daños e interferencias. La protección suministrada debe estar acorde con los riesgos identificados. Protección de los equipos contra las amenazas físicas y ambientales. La protección del equipo es necesaria para reducir el riesgo de acceso no autorizado a la información y su protección contra pérdida o robo. Así mismo, se debe considerar la ubicación y eliminación de los equipos. Se pueden requerir controles especiales para la protección contra amenazas físicas y para salvaguardar servicios de apoyo como energía eléctrica e infraestructura del cableado.
Métrica	Informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes. Número de chequeos (a personas a la salida y a existencias en stock) realizados en el último mes y porcentaje de chequeos que evidenciaron movimientos no autorizados de equipos o soportes informáticos u otras cuestiones de seguridad.

Fuente: Cervantes
Elaborado por: Ma. Lorena Valle & Jose L. Morales

- **Comunicación / Administración de Operaciones:** procedimientos en caso de accidente, plan de recuperación, definición de niveles de servicio y tiempo de recuperación, protección contra programas ilegales, etc.

TABLA N° 6 COMUNICACIÓN / ADMINISTRACIÓN DE OPERACIONES

Objetivo	Procedimientos y responsabilidades de: operación, gestión de servicios de terceras partes, planificación y aceptación del sistema, protección contra software malicioso, backup, gestión de seguridad de redes, utilización de soportes de información, intercambio de información y software, servicios de comercio electrónico y monitorización.
Principios	Se deben establecer responsabilidades y procedimientos para la gestión y operación de todos los recursos para el tratamiento de la información. Segregación de tareas cuando sea adecuado, para reducir el riesgo de un mal uso del sistema deliberado o por negligencia. La organización debe verificar la implementación de

	acuerdos, el monitoreo de su cumplimiento y gestión de los cambios con el fin de asegurar que los servicios que se ser prestan cumplen con todos los requerimientos acordados con los terceros. Se requiere una planificación y preparación avanzadas para garantizar la adecuada capacidad y recursos con objeto de mantener la disponibilidad de los sistemas requerida. Realizar proyecciones de los requisitos de capacidad en el futuro para reducir el riesgo de sobrecarga de los sistemas. Se deben establecer, documentar y probar, antes de su aceptación, los requisitos operacionales de los nuevos sistemas. Se requiere de ciertas precauciones para prevenir y detectar la introducción de código malicioso y códigos móviles no autorizados. Los usuarios deben conocer los peligros que puede ocasionar el software malicioso o no autorizado y los administradores deberían introducir controles y medidas especiales para detectar o evitar su introducción. Implante procedimientos de backup y recuperación que satisfaga sólo requisitos contractuales sino también requisitos de negocio "internos" de la organización. Decidir y establecer el tipo de almacenamiento, soporte a utilizar, aplicación de backup, frecuencia de copia y prueba de soportes. Encriptar copias de seguridad y archivos que contengan datos sensibles o valiosos.
Métrica	Métricas de madurez de procesos TI relativos a seguridad, tales como el semiperiodo de aplicación de parches de seguridad (tiempo que ha llevado parchear al menos la mitad de los sistemas vulnerables -esta medida evita la cola variable provocada por los pocos sistemas inevitables que permanecen sin parchar por no ser de uso diario, estar normalmente fuera de la oficina o cualquier otra razón).Costo del tiempo de inactividad debido al incumplimiento de los acuerdos de nivel de servicio. Evaluación del rendimiento de proveedores incluyendo la calidad de servicio, entrega, costo, etc. Porcentaje de cambios de riesgo bajo, medio, alto y de emergencia. Número y tendencia de cambios revertidos y rechazados frente a cambios exitosos. Porcentaje de sistemas (a) Que deberían cumplir con estándares de seguridad básica o similar y (b) Cuya conformidad con dichos

	estándares ha sido comprobada mediante benchmarking o pruebas. Tendencia en el número de virus, gusanos, troyanos o spa detectados y bloqueados. Número y costes acumulados de incidentes por software malicioso. Porcentaje de operaciones de Backus exitosas. Porcentaje de recuperaciones de prueba exitosas. Tiempo medio transcurrido desde la recogida de los soportes de backup de su almacenamiento fuera de las instalaciones hasta la recuperación exitosa de los datos en todas ubicaciones principales.

Fuente: Cervantes
Elaborado por: Ma. Lorena Valle & Jose L. Morales

- **Control de Acceso:** establecimiento de controles de acceso a diferentes niveles (sistemas, redes, edificios, etc.).

TABLA N° 7 CONTROL DE ACCESO

Objetivo	Requisitos de negocio para el control de accesos, gestión de acceso de usuario, responsabilidades del usuario, control de acceso en red, control de acceso al sistema operativo, control de acceso a las aplicaciones e informaciones, informática y conexión móvil.
Principios	Control de los accesos a la información, los recursos de tratamiento de la información y los procesos de negocio en base a las necesidades de seguridad y de negocio de la Organización. Para las regulaciones para el control de los accesos se deben considerar las políticas de distribución de la información y de autorizaciones. Establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información. Los procedimientos deben cubrir todas la etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información. Se debe prestar especial atención, si fuera oportuno, a la necesidad de controlar la asignación de permisos de acceso con privilegios que se salten y anulen la eficacia de los controles del sistema. Los usuarios deben ser conscientes de sus responsabilidades en el mantenimiento de controles de acceso eficaces, en particular

	respecto al uso de contraseñas y seguridad en los equipos puestos a su disposición. Implantar una política para mantener mesas de escritorio y monitores libres de cualquier información con objeto de reducir el riesgo de accesos no autorizados o el deterioro de documentos, medios y recursos para el tratamiento de la información. Control de los accesos a servicios internos y externos conectados en red. El acceso de los usuarios a redes y servicios en red no debe comprometer la seguridad de los servicios en red si se garantizan: a) Que existen interfaces adecuadas entre la red de la Organización y las redes públicas o privadas de otras organizaciones; b) Que los mecanismos de autenticación adecuados se aplican a los usuarios y equipos; c) El cumplimiento del control de los accesos de los usuarios a los servicios de información. Utilizar las prestaciones de seguridad del sistema operativo para permitir el acceso exclusivo a los usuarios autorizados. Las prestaciones deberían ser capaces de: a) La autenticación de los usuarios autorizados, de acuerdo a la política de control de accesos definida; b) Registrar los intentos de autenticación correctos y fallidos del sistema; c) Registrar el uso de privilegios especiales del sistema; d) Emitir señales de alarma cuando se violan las políticas de seguridad del sistema; e) Disponer los recursos adecuados para la autenticación; f) Restringir los horarios de conexión de los usuarios cuando sea necesario. Utilizar dispositivos de seguridad con objeto de restringir el acceso a las aplicaciones y sus contenidos. Restringir el acceso lógico a las aplicaciones software y su información únicamente a usuarios autorizados. Los sistemas de aplicación deben: a) Controlar el acceso de los usuarios a la información y funciones de los sistemas de aplicaciones, en relación a la política

	de control de accesos definida; b) Proporcionar protección contra accesos no autorizados derivados del uso de cualquier utilidad, software del sistema operativo y software malicioso que puedan traspasar o eludir los controles del sistema o de las aplicaciones; c) No comprometer otros sistemas con los que se compartan recursos de información. Tener políticas claramente definidas para la protección, no sólo de los propios equipos informáticos portátiles (es decir, laptops, PDAs, etc.), sino, en mayor medida, de la información almacenada en ellos. Por lo general, el valor de la información supera con mucho el del hardware. Asegurar que el nivel de protección de los equipos informáticos utilizados dentro de las instalaciones de la organización tiene su correspondencia en el nivel de protección de los equipos portátiles, en aspectos tales como antivirus, parches, actualizaciones, software cortafuegos, etc.
Métrica	Porcentaje de sistemas y aplicaciones corporativas para los que los "propietarios" adecuados han: (a) Sido identificados, (b) Aceptado formalmente sus responsabilidades, (c) Llevado a cabo -o encargado- revisiones de accesos y seguridad de aplicaciones, basadas en riesgo y (d) Definido las reglas de control de acceso basadas en roles. Tiempo medio transcurrido entre la solicitud y la realización de peticiones de cambio de accesos y número de solicitudes de cambio de acceso cursadas en el mes anterior. Porcentaje de descripciones de puesto de trabajo que incluyen responsabilidades en seguridad de la información: (a) Totalmente documentadas y (b) Formalmente aceptadas. Estadísticas de cortafuegos, tales como porcentaje de paquetes o sesiones salientes que han sido bloqueadas (por ejemplo intentos de acceso a páginas web prohibidas; número de ataques potenciales de hacking repelidos, clasificados en insignificantes/preocupantes/críticos). Estadísticas de vulnerabilidad de sistemas y redes, como número de vulnerabilidades conocidas cerradas, abiertas y nuevas;

	velocidad media de parcheo de vulnerabilidades (analizadas por prioridades/categorías del fabricante o propias). Porcentaje de plataformas totalmente conformes con los estándares de seguridad básica (comprobado mediante pruebas independientes), con anotaciones sobre los sistemas no conformes. Un informe sobre el estado actual de la seguridad de equipos informáticos portátiles (laptops, PDAs, teléfonos móviles, etc.), y de teletrabajo (en casa de los empleados, fuerza de trabajo móvil),con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo creciente, despliegue de configuraciones seguras, antivirus, firewalls personales, etc.

Fuente: Cervantes
Elaborado por: Ma. Lorena Valle & Jose L. Morales

- **Desarrollo y mantenimiento del sistema:** consideración de la seguridad en sistemas desde el diseño hasta el mantenimiento.

TABLA N° 8 DESARROLLO Y MANTENIMIENTO DEL SISTEMA

Objetivo	Requisitos de seguridad de los sistemas de información; procesamiento correcto en aplicaciones; controles criptográficos; seguridad de los ficheros del sistema; seguridad en los procesos de desarrollo y soporte; gestión de vulnerabilidades técnicas. (Garantizar la seguridad integral de los sistemas)
Principios	El diseño e implantación de los sistemas de información que sustentan los procesos de negocio pueden ser cruciales para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados previamente al desarrollo y/o implantación de los sistemas de información. Todos los requisitos de seguridad deben identificarse en la fase de recogida de requisitos de un proyecto y ser justificados, aceptados y documentados como parte del proceso completo para un sistema de información. Diseñar controles apropiados en las propias aplicaciones, incluidas las desarrolladas por los propios usuarios, para asegurar el procesamiento correcto de la información. Estos controles deben incluir la validación de los datos de entrada, el tratamiento interno y los datos de salida. Pueden ser requeridos controles

	adicionales para los sistemas que procesan o tienen algún efecto en activos de información de carácter sensible, valioso o crítico. Dichos controles deben ser determinados en función de los requisitos de seguridad y la estimación del riesgo. Desarrollar una política de uso de controles criptográficos. Establecer una gestión de claves que de soporte al uso de técnicas criptográficas. Controlar el acceso a los sistemas de ficheros y código fuente de los programas. Los proyectos TI y las actividades de soporte deben ser dirigidos de un modo seguro. Evitar la exposición de datos sensibles en entornos de prueba. Controlar estrictamente los entornos de desarrollo de proyectos y de soporte. Los directivos responsables de los sistemas de aplicaciones deben ser también responsables de la seguridad del proyecto o del entorno de soporte. Ellos deben garantizar que todas las propuestas de cambio en los sistemas son revisadas para verificar que no comprometen la seguridad del sistema o del entorno operativo
Métrica	Porcentaje de sistemas para los cuales los controles de validación de datos se han (a) Definido e (b) Implementado y demostrado eficacia mediante pruebas. Porcentaje de sistemas que contienen datos valiosos o sensibles para los cuales se han implantado totalmente controles criptográficos apropiados (periodo de reporte de 3 a 12 meses).Porcentaje de sistemas evaluados de forma independiente como totalmente conformes con los estándares de seguridad básica aprobados, respecto a aquellos que no han sido evaluados, no son conformes o para los que no se han aprobado dichos estándares. Estado de la seguridad en sistemas en desarrollo, es decir, uniforme sobre el estado actual de la seguridad en los procesos de desarrollo de software, con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo creciente, etc.

Fuente: Cervantes
Elaborado por: Ma. Lorena Valle & Jose L. Morales

- **Plan de continuidad empresarial:** definición de necesidades en términos de disponibilidad, recuperación de tiempo y establecimiento de ejercicios de emergencia.

TABLA N° 9 PLAN DE CONTINUIDAD EMPRESARIAL

Objetivo	Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a desastres o grandes fallos de los sistemas de información.
Principios	Implantar un proceso de gestión de continuidad del negocio para reducir, a niveles aceptables, la interrupción causada por los desastres y fallos de seguridad (que, por ejemplo, puedan resultar de desastres naturales, accidentes, fallas de equipos o acciones deliberadas) mediante una combinación de controles preventivos y de recuperación. Identificar los procesos críticos de negocio e integrar los requisitos de gestión de la seguridad de información para la continuidad del negocio con otros requisitos de continuidad relacionados con dichos aspectos como operaciones, proveedores de personal, materiales, transporte e instalaciones. Analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales. La seguridad de información debe ser una parte integral del plan general de continuidad del negocio y de los demás procesos de gestión dentro de la organización. La gestión de la continuidad del negocio debe incluir adicionalmente al proceso de evaluación, controles para la identificación y reducción de riesgos, limitar las consecuencias de incidencias dañinas y asegurar la reanudación a tiempo de las operaciones esenciales. Mantenimiento de una política de seguridad de la información para toda la organización.
Métrica	Porcentaje de planes de continuidad de negocio en cada una de las fases del ciclo de vida (requerido / especificado / documentado / probado). Porcentaje de unidades organizativas con planes de continuidad de negocio que han sido adecuadamente (a) Documentados y (b) Probados mediante test apropiados en los últimos 12 meses.

Fuente: Cervantes
Elaborado por: Ma. Lorena Valle & Jose L. Morales

- **Cumplimiento Legal:** respeto por la propiedad intelectual, las leyes y las reglamentaciones de la compañía.

TABLA N° 10 CUMPLIMIENTO LEGAL

Objetivo	Evitar incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad.
Principios	Los requisitos legales específicos deben ser advertidos por los asesores legales de la organización o por profesionales adecuadamente calificados. Los requisitos que marca la legislación cambian de un país a otro y pueden variar para la información que se genera en un país y se transmite a otro país distinto (por ej., flujos de datos entre fronteras). Realizar revisiones regulares de la seguridad de los sistemas de información. Las revisiones se deben realizar según las políticas de seguridad apropiadas y las plataformas técnicas y sistemas de información deberían ser auditados para el cumplimiento de los estándares adecuados de implantación de la seguridad y controles de seguridad documentados. Deben existir controles para proteger los sistemas en activo y las herramientas de auditoría durante el desarrollo de las auditorías de los sistemas de información. También se requiere la protección para salvaguardar la integridad y prevenir el mal uso de las herramientas de auditoría.
Métrica	Número de cuestiones o recomendaciones de cumplimiento legal, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de requisitos externos clave que, mediante auditorías objetivas o de otra forma admisible, han sido considerados conformes. Número de cuestiones o recomendaciones de política interna y otros aspectos de cumplimiento, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de revisiones de cumplimiento de seguridad de la información sin incumplimientos sustanciales. Número de cuestiones o recomendaciones de auditoría, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de hallazgos de auditoría relativos a seguridad de la información que han sido resueltos y cerrados, respecto al total de abiertos en el mismo periodo. Tiempo medio real de resolución/cierre de recomendaciones, respecto a los plazos acordados por la dirección al final de las auditorías.

Fuente: Cervantes
Elaborado por: Ma. Lorena Valle & Jose L. Morales

CAPÍTULO III

3. MARCO METODOLÓGICO

A fin de obtener los mejores resultados posibles en el presente trabajo de auditoría, se procedió a utilizar las siguientes técnicas y procedimientos:

3.1 IDEA A DEFENDER

Si se aplica una Auditoría Informática de la Seguridad de la Información mediante las normas ISO/IEC 17799, en la Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo (REFICH), las vulnerabilidades existentes en la seguridad de la información se evidenciaran y se evaluará el nivel de control de la Seguridad de la Información del Departamento de Control y Monitoreo.

3.2. TIPO DE INVESTIGACIÓN

Para poder realizar la Auditoría Informática de la Seguridad de la Información mediante las normas ISO/IEC 17799, debemos tener un amplio conocimiento del proceso de la información de la Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo (REFICH),el enfoque de esta investigación es mixto porque se realizará de forma cualitativa ya que se obtendrá información directa de lo investigado por medio de la aplicación de una entrevista; y de forma cuantitativa porque podemos determinar cuántos hallazgos hemos encontrado en la auditoría.

- ***EXPLORATORIO:*** Los mismos que facilitarán la realización de los procesos necesarios investigativos a utilizarse en este proyecto. Este método ha sido seleccionado de acuerdo al tipo de investigación que se está realizando.

- ***DESCRIPTIVO:*** La investigación a realizar es del nivel descriptiva, por cuanto se describe los conceptos de las normas ISO/IEC 17799, que facilita la auditoría informática, ya que proporciona el marco y la estructura para la consecución de los objetivos.

- ***EXPLICATIVA:*** Se explica su incidencia en que los indicadores se organizan en dos perspectivas, siendo una perspectiva de resultados (Perspectiva del Informe); y; una perspectiva Inductoras (Perspectiva de Procesos Internos).

3.3. MÉTODOS, TÉCNICAS E INSTRUMENTOS

El detalle o definir como se realizará la investigación, puntualiza la forma como se obtendrá la información y las actividades a realizar para conseguir los objetivos planteados. En el estudio se analizara seguridad en el sistema de información que maneja a la Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo, la Auditoría Informática de la Seguridad de la Información, las normas ISO/IEC 17799 que se inicia con la revisión histórica, bibliográfica y documental conocimiento que permite ejecutar la investigación en forma adecuada.

3.3.1 Métodos de Investigación

El proyecto a desarrollarse se basa en los siguientes métodos:

- **Método Deductivo:** Parte de las afirmaciones generales para llegar a conclusiones de carácter particular; la REFICH, dispone de un sistema de información que debe mantener una seguridad muy adecuada que permita llegar al socio con facilidad pero que tenga la protección adecuada que garantice y logre confianza de parte del socio.

- **El método Analítico:** Es un procedimiento riguroso formulado de manera lógica, para lograr la adquisición de conocimientos mediante la investigación de la forma como se maneja la información en la institución financiera.

3.3.2. Técnicas de Investigación

Las técnicas a utilizadas son:

- **Análisis Documental:** Este análisis se lo realizara al inventario que posee el área informática, respecto a sus recursos tecnológicos y a su vez del manual de funciones en el caso de tenerlo.

- **Entrevista:** Esta entrevista se lo realiza a una de las máximas autoridades de la Institución, en este caso al representante de la institución y responsable del área e implementos informáticos.

- **Encuesta:** La encuesta se lo realizara a las personas entrevistadas, la misma que eta establecida con una estructura lógica, rígida si cambia alguno en el trascurso del trabajo.

3.2.3 Instrumentos de Investigación

➢ **Cuestionario** El cuestionario dirigido a las personas entrevistadas consta de un máximo de 13 preguntas, mismas que estas determinas de una forma sencilla, clara con el fin de obtener la información y conocimientos necesarios para la Auditoría. **VER ANEXO N° 01…**

3.4 VERIFICACIÓN DE LA IDEA A DEFENDER

Después de aplicar la auditoría informática bajo la norma ISO/IEC 17799 en la Red de Estructura de Finanzas Populares y Solidarias de Chimborazo (REFICH), se ha evidenciado la vulnerabilidad existente en la Seguridad de la Información en el Departamento de Control y Monitoreo de la entidad los mismos que se reflejó después de hacer el análisis FODA y pasando a la evaluación del nivel de control interno mediante los cuestionarios aplicados en cada uno de los parámetros que indica la norma ISO/IEC 17799, y finalmente concluyendo con el informe de la auditoría las áreas críticas y sus respectivas recomendaciones.

Para un mejor entendimiento de que se planteó en el presente trabajo desarrollamos el siguiente cuadro en el cual observamos la utilización de la ISO, y damos a conocer las conclusiones que llegaron las entidades después de aplicar la Seguridad de la Información en las siguientes empresas:

TABLA N° 11 ADOPCIÓN DE LA NORMA ISO/IEC 17799 EN EL PAÍS

EMPRESAS	CONCLUSIONES
ANDINATEL	El plan desarrollado por la Ing. Mercedes Torres en el año 2007 fue conocida y evaluada por los directivos de Andinatel S.A., Vicepresidenta de Sistemas, Gerente de control informático, quienes a través de documentos adjuntos, indican que se ejecutó este plan de implementación de seguridad de la información y además se lo remitió a Contraloría Interna, tal trabajo conllevo una mejora en la seguridad de la información

	lo que represento una adopción total de la ISO.
CORPEI	Al adoptar la norma permitió aumentar la detección de riesgo de una empresa. Reducir la posibilidad del éxito agresor. Prevención en brechas de seguridad para actos criminales y violación de la seguridad.
COTECNA Certificadora Services Ltda.	La entidad adopta este sistema para que aborde la seguridad de la información de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización. ✓ Demuestra la garantía independiente de los controles internos y cumple los requisitos de gestión corporativa y de continuidad de la actividad comercial. ✓ Demuestra independientemente que se respetan las leyes y normativas que sean de aplicación. ✓ Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial. ✓ Verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información. ✓ Demuestra el compromiso de la cúpula directiva de su organización con la seguridad de la información. ✓ El proceso de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora

Fuente: Cuestionario aplicado al Departamento de Control y Monitoreo
Elaborado por: Ma. Lorena Valle &Jose L. Morales

Una vez expuesto las conclusiones de las empresas las cuales adoptaron la norma se determinó que este sistema conllevo a una mejora en la seguridad de la información detectando riesgos, posibilidad de éxito del agresor, actos criminales y violación de la información, lo que implicó en estas entidades la supervisión continua del rendimiento y mejora de la Seguridad de la Información.

CAPÍTULO IV

4. DESARROLLO DE LA AUDITORÍA INFORMÁTICA

4.1 Guía para Aplicar la Auditoría Informática para la Seguridad de la Información

4.1.1 Introducción

Antes de dar inicio al desarrollo de la Auditoría Informática es pertinente referirse de manera general, al proceso de Auditoría Informática. Al respecto indicamos lo siguiente:

A continuación se grafica el proceso de la Auditoría Informática, los pasos que debe seguir el auditor, en la realización del examen:

GRÁFICO N° 5 Proceso de Auditoría Informática

PROCESO DE AUDITORÍA INFORMÁTICA			
DIAGNÓSTICO GENERAL	**PLANIFICACIÓN**	**EJECUCIÓN**	**COMUNICACIÓN**

Elaborado por: Ma. Lorena Valle & Jose Morales

El proceso de Auditoría Informática es sistemático porque hay una interrelación indudable entre las diferentes fases que lo conforman, las mismas que son cuatro:

- **Diagnóstico General:** Conocimiento de la realidad de la entidad mediante el análisis F.O.D.A.

- **Planificación:** A partir de la autorización de la Orden de Trabajo de la Auditoría empezaremos con las siguientes planificaciones que son de dos tipos:

Preliminar.- en la que se analizará el conocimiento general de la entidad, datos generales, misión, visión, objetivos estratégicos, valores institucionales, base legal, estructura orgánica, autoridades y descripción del Departamento Control y Monitoreo.

Especifica.- breve análisis y explicación sobre antecedentes, motivos, objetivos, alcances, tiempo para la ejecución del trabajo, recursos a utilizarse, resultados obtenidos.

- **Ejecución.-** Es la realización de la Auditoría Informática, en esta fase se desarrolla en dos partes que son los siguientes:

Archivo Permanente.- *consta de la información general de la entidad, abreviatura y hojas de marca.*

Abreviaturas.- son las siglas que nos ayuda a identificar en que proceso estamos dentro de la Auditoria Informática.

Hojas de Marcas.- son los símbolos que vamos a ocupar en la ejecución, los mismos que nos ayudaran a identificar los hallazgos de la Auditoria Informática.

Archivo Corriente.- consta de los siguientes parámetros a revisar:

- Programa de auditoria
- Solicitud de Autorización
- Entrevista al Director Ejecutivo de la entidad.
- Principios de la Entidad
- Entrevista a la encargada del Departamento de Control y Monitoreo.

- **Comunicación.-** es la preparación del informe en el cual consta el hallazgo y recomendación.

Programa de Informe Final de auditoría

Informe de Auditoría.

4.1.2 Diagnóstico general

Este se basa en el conocimiento de la organización, es importante determinar los factores internos y externos que eventualmente afectan el desempeño de la entidad, conocer la relación que se mantiene con elementos del entorno próximo y remoto,

ayudan a definir potenciales oportunidades, amenazas, debilidades y fortalezas, lo que permite definir una estrategia de mejoramiento, que se incorporará luego como sugerencias de auditoría. Con la información y elementos obtenidos es factible obtener un conocimiento integral de la entidad desde un punto de vista sistemático, nos permitirá entender el funcionamiento de la organización desde la recepción de información hasta la entrega de los resultados de los monitoreos y su posterior impacto a la entidad.

4.1.3 Planificación de Auditoría

La planificación de la auditoría comporta el desarrollo de una estrategia global en base al objetivo y alcance del encargo y la forma en que se espera que responda la organización de la entidad, el auditor debe considerar, entre otras cuestiones, las siguientes:

- Una adecuada comprensión del negocio de la entidad, del sector en que ésta aplica.

En la fase de planificación deben quedar totalmente aclaradas las siguientes cuestiones:

- *¿Dónde se va a realizar el trabajo?*
- *¿Cuándo o en qué período de tiempo se va a realizar?*
- *¿En qué fecha es necesario que esté terminado el trabajo?*
- *¿Cuándo estará terminado el informe?*

El auditor deberá documentar adecuadamente el plan de la auditoría, en el que cabe diferenciar: análisis general del riesgo, plan global de auditoría y la redacción y utilización de programas de auditoría.

4.1.3.1 Planificación Preliminar.- La planificación preliminar nos permite obtener una visión global de la entidad; conocer las principales actividades, metas y objetivos, análisis general de la información y decidir en forma preliminar los componentes. Incluye, entre otros los siguientes elementos:

- Conocimiento de la Institución

- Misión
- Visión
- Objetivos Estratégicos
- Valores Institucionales
- Base legal
- Estructura Orgánica
- Autoridades de la entidad
- Descripción del Departamento de Control y Monitoreo

4.1.3.2 Planificación específica.-Se debe considerar la recopilación de información, identificación y realización de pruebas de auditoría, incluyendo, si se acuerda, análisis de vulnerabilidad de aplicaciones. Para la planificación específica, se debe incluir los siguientes elementos:

- Utilizar la información importante de la planificación preliminar
- Determinar el departamento a evaluar.
- Elaborar los Programas de trabajo

Según León M. (2013), uno de los elementos fundamentales de la planificación específica es las clases de riesgos y los programas de auditoría.

Riesgo inherente: Se relaciona con la naturaleza propia del rubro evaluado. Lo afectan factores como el volumen de operaciones, la experiencia del personal contable, la Significatividad del componente y observaciones de auditorías anteriores.

Riesgo de control: Tiene relación directa con el funcionamiento de los controles internos. A mayor confianza en los controles menor riesgo de control y viceversa.

Riesgo de detección: Es la posibilidad de que pese a la aplicación de los procedimientos de auditoría no se detecten errores significativos. Los factores que lo

afectan son la experiencia de los auditores, la dotación de equipo informático y recursos suficientes.

“A MAYOR RIESGO INHERENTE Y DE CONTROL, SE DEBE DISMINUIR EL RIESGO DE DETECCIÓN”

La relación inversa es un resultado lógico de las circunstancias establecidas en la empresa auditada. Si las condiciones determinan un número significativo de operaciones con importancia monetaria y a esto se añaden debilidades en los controles definidos en los procesos, es evidente que se requiere un mayor esfuerzo de auditoría para minimizar el efecto de estos riesgos.

Con los resultados obtenidos se puede preparar el reporte de planificación específica, considerando el tiempo estimado para la ejecución del trabajo, la distribución de tareas y los procedimientos que deben aplicarse.

La metodología de determinación de riesgos, que se refirió en párrafos anteriores, nos permitirá definir el nivel de riesgo de control:

$$NC = CT * 100 / PT$$

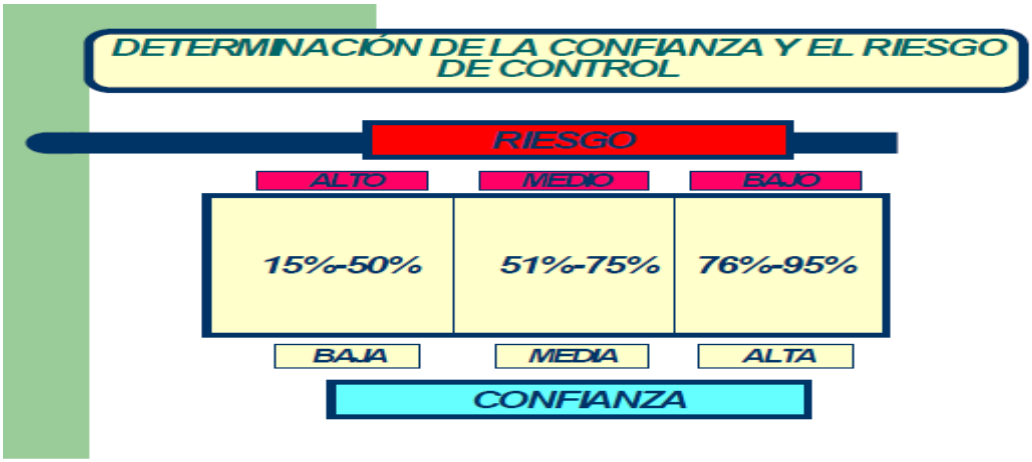
NC = Nivel de confianza

CT = Calificación total

PT = Ponderación

Por oposición a nivel de confianza obtenemos el riesgo de control así como lo señala el gráfico siguiente:

GRÁFICO N° 6 Determinación de la confianza y el riesgo de control.



Fuente: Manual de Auditoría Gubernamental (CGE)

PROGRAMAS DE AUDITORIA.- Este es el instrumento principal para la realización de la auditoría, ya que estos indican los procedimientos a seguir en referencia a los papeles de trabajo, quien lo realiza y supervisa, la fecha de ejecución de la cada uno de los procesos a realizar.

A continuación se presenta los modelos de Programas de Auditoría Informática a utilizar, basados en nuestra formación académica:

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

PROGRAMA DE AUDITORÍA- DIAGNÓSTICO GENERAL

N°	DESCRIPCIÓN	REF P/T	REALIZADO POR:	FECHA
	OBJETIVOS:			
1	Obtener la información y recursos necesarios para poder ejecutar auditoría informática de la seguridad de la información.			
2	Establecer las normas o leyes a las que esta sujetas a cumplir la Entidad.			
3	Establecer la Estructura Orgánica que posee la Entidad.			
	PROCEDIMIENTOS:			
1	Solicitar al Director Ejecutivo de la Entidad que nos proporcione la información y recursos necesarios para poder realizar el trabajo de Auditoria.			
2	Entrevistar al Director Ejecutivo de la Institución.			
3	Solicitar la Gestión Institucional y Principios que mantienen.			
4	Solicitar fundamentación teórica o bases institucionales.			

ELABORADO POR:	**FECHA:**
REVISADO POR:	**FECHA:**

MORALES & VALLE ASOCIADOS
AUDITORES INDEPENSIENTES CIA. LTDA

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

PROGRAMA DE AUDITORÍA- EVALUACIÓN DEL CONTROL INTERNO

N°	DESCRIPCIÓN	REF P/T	REALIZADO POR:	FECHA
	OBJETIVOS:			
1	Verificar el cumplimiento de las normas ISO/IEC 17799 sobre el uso de las Seguridad de la Información sujetas a cumplir la Entidad.			
2	Establecer la colaboración del personal de la entidad a fin de obtener información y conocimientos sobre las actividades que esta mantiene.			
3	Determinar la matriz de ponderación para asegurar el manejo correcto de los recursos.			
4	Determinar los aspectos críticos a través de la elaboración de hojas de hallazgos con sus conclusiones y recomendaciones respectivas.			
	PROCEDIMIENTOS:			
1	Elaboración del Plan de Auditoría de Control I			
2	Aplicar Cuestionarios de Control Interno			
2.1	Política de Seguridad			
2.2	Organización de Seguridad			
2.3	Calificación y control de activos			

ELABORADO POR:	**FECHA:**
REVISADO POR:	**FECHA:**

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

PROGRAMA DE AUDITORÍA- EVALUACIÓN DEL CONTROL INTERNO

N°	DESCRIPCIÓN	REF P/T	REALIZADO POR:	FECHA
2.4	Seguridad del Personal			
2.5	Seguridad Física y del entorno			
2.6	Comunicación/ Administración de Operaciones			
2.7	Control de Acceso			
2.8	Desarrollo y mantenimiento del sistema			
2.9	Plan de continuidad empresarial			
3	Evaluación de Riesgo			
3.1	Tabulación y Ponderación de Riesgo			
4	Elaboración de Hojas de Hallazgos			

ELABORADO POR:	**FECHA:**
REVISADO POR:	**FECHA:**

MORALES & VALLE ASOCIADOS
AUDITORES INDEPENSIENTES CIA. LTDA

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

PROGRAMA DE AUDITORÍA- COMUNICACIÓN DE RESULTADOS

N°	DESCRIPCIÓN	REF P/T	REALIZADO POR:	FECHA
	OBJETIVOS:			
1	Emitir las pertinentes conclusiones y recomendaciones en el informe de auditoría.			
	PROCEDIMIENTOS:			
1	Informe Final de Auditoría a la Gestión de las Tecnologías de la Información.			

ELABORADO POR:	**FECHA:**
REVISADO POR:	**FECHA:**

4.1.5 Ejecución del trabajo

En el transcurso de una auditoría, los auditores mantendrán constante comunicación con los ejecutivos y empleados de la entidad bajo examen, dándoles la oportunidad para presentar pruebas documentadas, así como información verbal pertinente respecto de los asuntos sometidos a examen, este trabajo lo desarrollaremos en dos partes que son los siguientes:

- ***Archivo Permanente.-*** *consta de la información general de la entidad, abreviatura y hojas de marca.*

- ***Archivo Corriente.-*** consta de los siguientes parámetros a revisar:

FASE I: DIAGNOSTICO GENERAL DE LA ENTIDAD

Programa de auditoria

Solicitud de Autorización

Entrevista al Director Ejecutivo de la entidad.

Principios de la Entidad

Entrevista de la encargada de control y monitoreo.

FASE II: CONTROL INTERNO

Memorando de Planeación

Programas de Auditoria de Auditoría de Control interno.

Cuestionarios de Control Interno.

Matriz de resultados de Control interno.

FASE III: EJECUCIÓN

Programa de Auditoría de Ejecución

Hoja de hallazgos.

FASE IV: COMUNICACIÓN DE RESULTADOS

Programa de Informe Final de auditoría

Informe de Auditoría.- El informe de Auditoría Informática constituye el producto final del trabajo del auditor, a través del cual, genera un valor agregado, que permitirá a la entidad auditada mejorar el desempeño de sus actividades.

Al finalizar la Auditoría Informática de la Seguridad de la Información, se presentan las conclusiones y recomendaciones basadas en los hallazgos examinados durante la ejecución del trabajo dirigido al Director Ejecutivo de la entidad, el mismo que tomará medidas correctivas en caso de su aceptación.

En base a la guía presentada aplicaremos nuestro trabajo de la siguiente manera siguiendo los pasos planteados:

4.2 DIAGNÓSTICO GENERAL

El presente análisis se ajusta a la situación actual de la Red de Estructura de Finanzas Populares y Solidarias de Chimborazo y en especial al Departamento de Control y Monitoreo, para obtener una información adecuada se utilizó la técnica FODA misma que permite visualizar la imagen – objeto, es decir, cómo se encuentra al momento.

4.2.1 Matriz Preliminar del FODA

TABLA N° 12 MATRIZ PRELIMINAR DEL FODA

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO "REFICH"	
FORTALEZAS	**DEBILIDADES**
F1. Cuenta con un sistema de seguridad contra incendios. **F2.** Trabajan dos personas en el departamento. **F3.** Se realiza mantenimiento correctivo al equipo. **F4.** Cuenta con contraseñas para la seguridad de la información **F5.** Existe personal con experiencia **F6.** Cuentan con licencias para el software utilizado.	**D1.** No cuenta con el suficiente equipo informático para cumplir con el trabajo departamental. **D2.** No cuenta con una debida planificación de capacitación del personal. **D3.** No cuenta con una adecuada infraestructura física. **D4**. El mobiliario no abastece para el desarrollo normal del trabajo en el departamento. **D5.** No existe un manual de control interno para el manejo de la información. **D6.** No se realiza mantenimiento preventivo a los equipos informáticos

	D7. No cuenta con designación de responsabilidades para el cuidado de la información

Fuente: Análisis FODA
Elaborado forma. Lorena Valle & Jose L. Morales

4.2.2 Matriz de Impacto o Incidencia

TABLA N° 13 MATRIZ DE IMPACTO O INCIDENCIA

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO "REFICH"	
FORTALEZAS	**IMPACTO O INCIDENCIA**
F1. Cuenta con un sistema de seguridad contra incendios. **F2.** Trabajan dos personas en el departamento. **F3.** Se realiza mantenimiento correctivo al equipo. **F4.** Cuenta con contraseñas para la seguridad de la información **F5.** Existe personal con experiencia **F6.** Cuentan con licencias para el software utilizado.	**F1.** Confianza por parte de los usuarios ya que el equipo de cómputo no está expuesto a riesgo de incendio. **F2.** Personal suficiente y competente para el trabajo a realizar en el departamento. **F3.** Perduración de los equipos tecnológicos. **F4.** Conservación y cuidado de la información utilizada por el departamento. **F5.** Trabajos realizados con eficiencia. **F6.** Se trabaja de manera normal e ininterrumpidamente.
DEBILIDADES	**IMPACTO O INCIDENCIA**
D1. No cuenta con el suficiente equipo informático para cumplir con el trabajo departamental. **D2.** No cuenta con una debida planificación de capacitación del personal. **D3.** No cuenta con una adecuada infraestructura física. **D4**. El mobiliario no abastece para el desarrollo normal del trabajo en el departamento. **D5**. No existe un manual de control interno para el manejo de la información. **D6.** No se realiza mantenimiento preventivo a los equipos informáticos **D7.** No cuenta con designación de responsabilidades para el cuidado de la información.	**D1.** No satisface las necesidades del personal del departamento. **D2.** Procesos de ejecución de trabajo antiguo e influencia en los informes de los mismos. **D3**. No satisface las necesidades del personal del departamento. **D4.** Conflictos internos en el trabajo normal del departamento. **D5**. Mal uso de los recursos informáticos. **D6**. Daños en los equipos informáticos. **D7.** Trabajo no confiable para los usuarios.
OPORTUNIDADES	**IMPACTO O INCIDENCIA**
OPORTUNIDADES **O1.** El avance tecnológico ofrece un	**OPORTUNIDADES** **O1.** Mejores programas para el trabajo departamental.

abanico de mejoras. **O2.** Auditorías externas. **O3**. Cursos de capacitaciones informáticas. **O4.** Reformas a las normas informáticas.	**O2.** La identificación de las vulnerabilidades a las que se encuentra sujeta el departamento. **O3.** Actualización en conocimientos teóricos y prácticos de los avances tecnológicos. **O4.** El uso correcto de cada recurso informático dentro del área.
AMENAZAS	**IMPACTO O INCIDENCIA**
AMENAZAS **A1.** Delincuencia en el sector. **A2.** Virus y aplicaciones maliciosas. **A3.** Cambio de gobierno ejecutivo. **A4.** Desastres naturales.	**AMENAZAS** **A1.** Daños en infraestructura y pérdidas de información y equipos. **A2.** Pérdidas de información. **A3.** Nuevos diseños de trabajo y estabilidad laboral. **A4.** Daño total y parcial de los equipos e información.

Fuente: Análisis FODA
Elaborado por: Ma. Lorena Valle & Jose L. Morales

4.2.3 Medios Internos

En esta matriz se califica a los medios internos (Fortalezas y Debilidades) que posee la Entidad, para la ponderación de nuestros factores el universo es igual a 1 el mismo que será dividido para el número de puntos encontrados en la encuesta los cuales se multiplicará por la calificación de acuerdo al rango del 1 al 5, cuyo resultado final en nos indicara en qué situación se encuentra el Departamento ante las Fortalezas y Debilidades.

4.2.3.1 Calificación de Medios Internos

TABLA N° 14 MEDIOS INTERNOS

CALIFICACIÓN	DESCRIPCIÓN
1	**Debilidad Mayor**
2	**Debilidad Menor**
3	**Equilibrio**
4	**Fortaleza Menor**
5	**Fortaleza Mayor**

Fuente: Análisis FODA
Elaborado por: Ma. Lorena Valle & Jose L. Morales

4.2.3.2 Matriz de Medios Internos

TABLA N° 15 MATRIZ DE MEDIOS INTERNOS

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO "REFICH"				
FORTALEZAS				
N°	**FACTOR INTERNO**	**PONDERACIÓN**	**CALIFICACIÓN**	**RESULTADO**
1	Cuenta con un sistema de seguridad contra incendios.	**0,07692**	**5**	**0,39**
2	Trabajan dos personas en el departamento.	**0,07692**	**5**	**0,39**
3	Se realiza mantenimiento correctivo al equipo.	**0,07692**	**3**	**0,23**
4	Cuenta con contraseñas para la seguridad de la información	**0,07692**	**3**	**0,23**
5	Existe personal con experiencia	**0,07692**	**4**	**0,31**
6	Cuentan con licencias para el software utilizado	**0,07692**	**4**	**0,31**
DEBILIDADES				
7	No cuenta con el suficiente equipo informático para cumplir con el trabajo departamental.	**0,07692**	**1**	**0,08**
8	No cuenta con una debida planificación de capacitación del personal.	**0,07692**	**2**	**0,15**
9	No cuenta con una adecuada infraestructura física.	**0,07692**	**3**	**0,23**
10	El mobiliario no abastece para el desarrollo normal del trabajo en el departamento	**0,07692**	**2**	**0,15**
11	No existe un manual de control interno para el manejo de la información	**0,07692**	**1**	**0,08**
12	No se realiza mantenimiento preventivo a los equipos informáticos	**0,07692**	**1**	**0,08**
13	No cuenta con designación de responsabilidades para el cuidado de la información	**0,07692**	**3**	**0,23**
	TOTAL	**1**	**37**	**2,86**

Fuente: Análisis FODA
Elaborado por: Ma. Lorena Valle & Jose L. Morales

4.2.3.3 Análisis de la Matriz de Medios Internos.- Una vez realizado el análisis en una escala del 1 al 5, se determinó como resultado una ponderación de 2,86 lo cual nos da a deducir que el departamento de control y monitoreo de la Entidad tiene más debilidades que fortalezas, por lo cual es importante mejorar internamente esta área bajo los siguientes aspectos: determinación por parte de la Entidad, de un mayor porcentaje de presupuesto al departamento, a fin de realizar mayores inversiones en infraestructura y recursos tecnológicos, realizar una nueva planificación de trabajo en la que conste la realización de manuales de control y de funciones para realizar un trabajo eficaz y eficiente.

4.2.4 Medios Externos

De la misma manera la matriz de los medios externos (Oportunidades y Amenazas) que posee la Entidad, para la ponderación de nuestros factores el universo es igual a 1 el mismo que será dividido para el número de puntos encontrados en la encuesta los cuales se multiplicará por la calificación de acuerdo al rango del 1 al 5, cuyo resultado final en nos indicara en qué situación se encuentra el Departamento ante las Oportunidades y Amenazas.

4.2.4.1 Calificación de Medios Externos

TABLA N° 16 MEDIOS EXTERNOS

CALIFICACIÓN	DESCRIPCIÓN
1	**Amenaza Mayor**
2	**Amenaza Menor**
3	**Equilibrio**
4	**Oportunidad Menor**
5	**Oportunidad Mayor**

Fuente: Análisis FODA
Elaborado por: Ma. Lorena Valle & Jose L. Morales

4.2.4.2 Matriz De Medios Externos

TABLA N° 17 MATRIZ DE MEDIOS EXTERNOS

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO "REFICH"				
OPORTUNIDADES				
N°	**FACTOR EXTERNO**	**PONDERACIÓN**	**CALIFICACIÓN**	**RESULTADO**
1	El avance tecnológico ofrece un abanico de mejoras.	**0.125**	**5**	**0.625**
2	Auditorías externas.	**0.125**	**5**	**0.625**
3	Cursos de capacitaciones informáticas.	**0.125**	**4**	**0.5**
4	Reformas a las normas informáticas.	**0.125**	**4**	**0.5**
AMENAZAS				
5	Delincuencia en el sector.	**0.125**	**2**	**0.25**
6	Virus y aplicaciones maliciosas	**0.125**	**3**	**0.375**
7	Cambio de gobierno ejecutivo.	**0.125**	**1**	**0.125**
8	Desastres naturales.	**0.125**	**3**	**0.375**
	Total	**1**	**27**	**3.38**

Fuente: Análisis FODA
Elaborado por: Ma. Lorena Valle & Jose L. Morales

4.2.4.3 Análisis De La Matriz De Medios Externos

Una vez realizado el análisis en una escala del 1 al 5 a los medios externos se determinó una ponderación de 3,38 lo cual nos da a deducir que Departamento de Control y Monitoreo mantiene un equilibrio en relación a sus oportunidades y amenazas, debido a que esta Entidad posee capitales y planificaciones de Fundaciones relacionadas a la economía solidaria mismas que son dirigidas por la Asamblea General de Socios.

4.3 ORDEN DE TRABAJO

ORDEN DE TRABAJO N° 001

Riobamba, 03 de marzo del 2014

Ing. Edwin Niamiña Lara

DIRECTOR EJECUTIVO DE LA RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO.

De mis consideraciones

Mediante la presente me dirijo a usted para solicitarle de la manera más comedida, autorice la realización de la **AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN BAJO LAS NORMAS ISO/IEC 17799, EN LA RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO (REFICH). PERIODO 2012,** la misma que se la desarrollará de acuerdo a las ***NORMASISO/IEC 17799*** emitidas por la Organización Internacional de Estandarización.

Los objetivos de esta Auditoría están encaminados a evaluar del grado de eficiencia y efectividad del sistema de control interno que la Entidad tiene sobre los sistemas informáticos, así como la verificar el cumplimiento de disposiciones legales, reglamentarias y normativas, los resultados se darán a conocer a través del informe de auditoría emitido al final de este trabajo, mismo que incluirá comentarios, conclusiones y recomendaciones.

Atentamente

Ma. Lorena Valle Romero.
SUPERVISOR

4.4 PLANIFICACIÓN

4.4.1 Planificación Preliminar

4.4.1.1 Conocimiento de la Institución.

REFICH se constituye como una organización de segundo piso que apoya, coordina y ejecuta procesos alternativos de intermediación financiera con Estructuras Financieras Populares y Locales en la provincia de Chimborazo, que fomenta la unión, responsabilidad, confianza y la solidaridad de sus 18 Filiales ubicada en los cantones: Alausí, Pallatanga, Colta, Guamote, Riobamba, Chambo, Guano y Chunchi.

Considerada por sus Filiales como un espacio democrático de integración y cooperación mutua entre cooperativas, cajas de ahorro y crédito y grupos asociativos, creada para fortalecer el trabajo de las Estructuras Financieras Locales filiales que son actores indiscutibles de la Economía Popular y Solidaria, a través de la capacitación, asistencia técnica y asesoramiento, comprometidos con el Desarrollo Económico Local de las comunidades, parroquias y cantones a los que pertenecen.

La Personería Jurídica a REFICH fue emitida por el Ministerio de Industrias y Productividad (MIPRO), en la ciudad de Ambato, Acuerdo Ministerial No. 09432 con fecha del 25 de noviembre de 2009, después de haber cumplido con todos los requisitos legales para la adjudicación de la Personería Jurídica.

4.4.1.2 Misión

"La Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo es una organización integradora conformada por Estructuras Financieras Locales que tienen objetivos comunes y basa su trabajo en principios y valores, articulando servicios financieros y no financieros entre sus filiales, impulsando el desarrollo socio-económico de la provincia con representatividad local e incidencia nacional".

4.4.1.3 Visión

"Al 2015 la Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo es una organización ética, social y financieramente sostenible que promueve el desarrollo socio económico de los territorios rurales y urbano marginales de la provincia

brindando servicios financieros y no financieros de calidad que responden a las necesidades y oportunidad de sus filiales".

4.4.1.4 Objetivos Estratégicos

4.4.1.4.1 Objetivos Generales

- Mejorar representatividad de sus filiales dentro de la estructura del directorio de REFICH, para garantizar la participación equitativa en la toma de decisiones.

- Afianzar las relaciones de las filiales para garantizar el empoderamiento y compromiso en la gestión socio organizativo de la REFICH.

4.4.1.4.2 Objetivos Específicos

- Consolidar la información en base a criterios de la pertinencia en la agrupación de las variables proporcionadas.

- Mantener estadísticamente la información de las Filiales de REFICH como un capital tangible y estratégico de fluidez informativa.

- Determinar las Fortalezas, Oportunidades, Debilidades y Amenazas del universo de REFICH localizando las principales variables a ser atendidas para la presentación de propuestas y proyectos técnicos para mitigar o afianzar procesos de fortalecimiento.

4.4.1.5 Valores Institucionales

La Entidad cuenta con un recurso humano que practica los valores de:

- Identidad
- Disciplina
- Transparencia
- Compromiso
- Solidaridad
- Respeto
- Puntualidad
- Honestidad

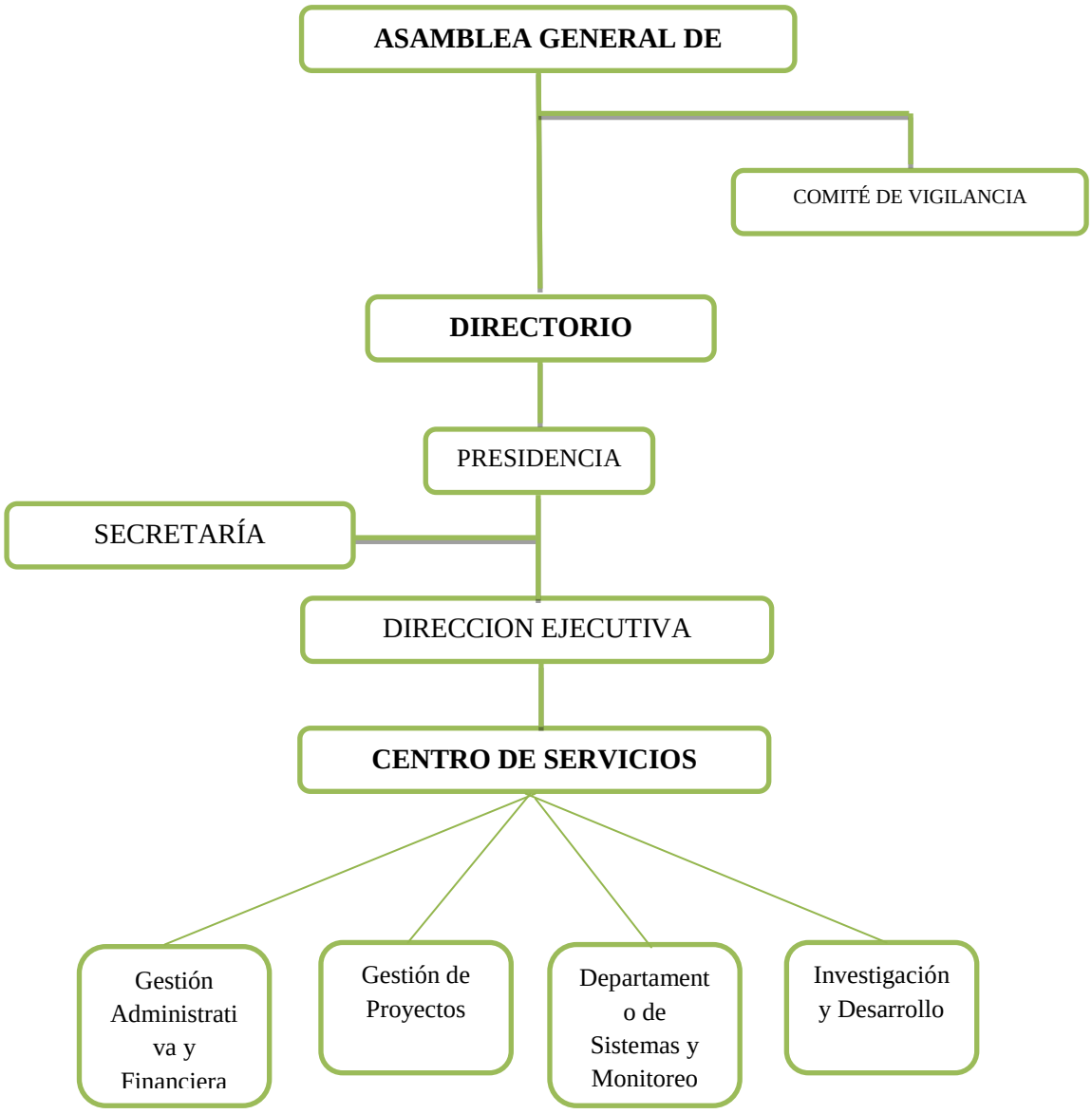
- Cordialidad

4.4.1.6 Base legal

La Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo REFICH, adquirió su personería jurídica en noviembre 2009, mediante Acuerdo Nº 03492 del Ministerio de Industrias y Productividad (MIPRO). Como red se integró con IFIPS socias ubicadas en los cantones de Alausí, Pallatanga, Colta, Guamote, Riobamba, Chambo, Cumanda, Guano y Chunchi.

4.4.1.7 Estructura Orgánica de la Entidad

GRÁFICO N° 7: Estructura Orgánica de la Entidad



4.4.1.7 Autoridades de la Entidad

Presidenta: Ing. Carmen Cecilia Uvidia

Director Ejecutivo: Ing. Edwin Ñamiña Lara

DEPARTAMENTO DE CONTROL Y MONITOREO

Técnico 1: Ing. María Lorena Moreno

Técnico 2: Ing. Olger Sarango Lapo

4.4.1.9 Descripción del Departamento de Control y Monitoreo

El Departamento de Control y Monitoreo dentro de la Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo, fue creada debido a la gran cantidad de información que se genera de las cajas y bancos comunales y para un debido y correcto manejo de la misma deberá estar en concordación con los avances y desarrollos tecnologías.

Inicialmente la entidad contaba una sola persona en el departamento, acorde a la capacidad que prestaba el espacio fisco del departamento, debido al incremento de trabajo se amplió el departamento y una persona más que realizara las mismas funciones para satisfacer las necesidades de la entidad

4.4.2 Planificación Específica

4.4.2.1 Datos Generales

UBICACIÓN: Riobamba - Ecuador
ENTIDAD: Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo
PROVINCIA: Chimborazo.
CANTON: Riobamba.
PARROQUIA: Lizarzaburo
DIRECCIÓN: Río Chanchan 18-33 entre Chile y Villarroel
TELEFONO: 032-941-459
TIPO DE TRABAJO: Auditoría Informática de la seguridad de la información.
FECHA DE INICIACIÓN: 03 de Marzo de 2014

4.4.2.2. Antecedentes de la Auditoría

La Auditoría Informática de la Seguridad de la Información, En la Red de Estructura de Finanzas Populares y Solidarias de Chimborazo (REFICH), Periodo 2012, se realizará aplicando la Norma 17799 de la Organización Internacional de Estandarización.

4.4.2.3 Motivos de la Auditoría

La presente auditoría se realizara de acuerdo a la orden de trabajo N°001 con fecha 03 de Marzo de 2014, misma que se ejecutara una vez entregada la orden.

4.4.2.4 Objetivos de la Auditoría

Desarrollar una Auditoría Informática de la Seguridad de la Información basada en la norma ISO/IEC 17799 con la finalidad de plantear las medidas y controles que mejoren las operaciones del Departamento de Control y Monitoreo en la Red de Estructura de Finanzas Populares y Solidarias de Chimborazo (REFICH), periodo 2012.

- Realizar un análisis bibliográfico documental respecto a la Auditoria Informática, sistema de información y la norma ISO/IEC 17799 como elementos que direccionen la investigación.

- Evaluar el Sistema de Información en la Red de Estructura de Finanzas Populares y Solidarias de Chimborazo aplicando la norma ISO/IEC 17799.

- Emitir informe de auditoría con recomendaciones para el mejoramiento del Departamento de Control y Monitoreo.

4.4.2.5 Alcance de la Auditoría

La Auditoría Informática de la Seguridad de la Información, es la revisión y la evaluación de los controles internos, sistemas, procedimientos y equipos informáticos, su eficiencia y seguridad, de la organización de los procesamientos de la información, con la finalidad de lograr una utilización más eficiente y segura, que servirá para una adecuada toma de decisiones dentro del Departamento de Control y Monitoreo en la Entidad.

4.4.2.6 Tiempo para la ejecución del trabajo

La Auditoría de la Seguridad de la Información de la Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo se realizara en 120 días.

4.4.2.7 Recursos a Utilizarse

RECURSOS HUMANOS

- ✓ **SUPERVISOR:** María Lorena Valle Romero
- ✓ **AUDITOR:** Jose Luis Morales Garcés

RECURSOS MATERIALES

- ✓ Laptop
- ✓ Impresora
- ✓ Lápiz y bicolor
- ✓ Borrador
- ✓ Hojas de papel bond
- ✓ Cámara de fotos
- ✓ Carpetas
- ✓ Calculadora

4.4.2.8 Resultados Obtenidos

Una vez obtenido los resultados, se emitirá el informe de auditoría con sus respectivas recomendaciones y conclusiones para la tome de acciones correctivas de acuerdo a los hallazgos encontrados para que sean tomados en cuenta por la Entidad

.

Srta. Ma. Lorena Valle Romero — **SUPERVISOR**

Sr. Jose L. Morales Garcés — **AUDITOR**

4.5 Cronograma

En la siguiente tabla indicamos el tiempo esperado para cada actividad en semanas.

TABLA N° 18 CRONOGRAMA DE AUDITORÍA

N°	ACTIVIDADES A DESARROLLAR	MARZO 2014 – JUNIO 2014															
		MARZO 2014				ABRIL 2014				MAYO 2014				JUNIO 2014			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	**PLANIFICACIÓN**																
2	***Cronograma de Auditoría***																
3	***Orden de Trabajo***																
4	**PLANIFICACIÓN PRELIMINAR**																
5	**PLANIFICACIÓN ESPECÍFICA**																
6	***Memorándum***																
7	***Programas de Trabajo***																
8	***Papeles de Trabajo***																
9	**EVALUACIÓN DEL SISTEMA CONTROL INTERNO**																
10	***Evaluación de Riesgo***																
11	**ELABORACIÓN DE HALLAZGOS**																
12	***Hallazgos relevantes***																
13	**ELABORACIÓN DEL DICTÁMEN DE AUDITORÍA**																
14	**CONCLUSIONES Y RECOMENDACIONES**																

Elaborado: Ma. Lorena Valle R. & Jose L. Morales

4.6. EJECUCIÓN

4.6.1 Archivo Permanente

MORALES & VALLE
ASOCIADOS
AUDITORES INDEPENSIENTES CIA. LTDA

ARCHIVO PERMANENTE

MORALES & VALLE ASOCIADOS
AUDITORES INDEPENSIENTES CIA. LTDA

AP

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

MARZO – MAYO 2014

INDICE

ELABORADO POR:	J.M	**FECHA:**	11-03-2014
REVISADO POR:	M.V	**FECHA:**	18-03-2014

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

VISITA PRELIMINAR

OBJETIVO DE LA VISITA PRELIMINAR: Realizar observaciones, indagaciones, solicitar y recopilar toda la información necesaria para verificar el cumplimiento de las Normas de I.S.O 17799 que la Entidad tiene sobre las Seguridad de la Información.

1.- ENTIDAD: Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo

2.- FECHA DE CREACION DE LA ENTIDAD: Noviembre 2009

3.- DIRECCIÓN: Río Chanchan 18-33 entre Chile y Villarroel

4.- PROVINCIA: Chimborazo.

5.- CANTON: Riobamba.

6.- PARROQUIA: Lizarzaburo

7. -HORARIO DE ATENCIÓN:

8:30 am - 12:30 am

13:30am - 17:30 am

8. - TELÉFONOS: 032941-459

9.- SERVICIOS INSTITUCIONALES:

- Análisis financieros.
- Fortalecimientos Técnicos mediante indicadores.
- Contabilidad.
- Capacitaciones y Actualizaciones del medio.
- Soporte Técnico y aplicaciones de sistemas informáticos.

INFORMACIÓN GENERAL

RESEÑA HISTÓRICA

La Personería Jurídica a REFICH fue emitida por el Ministerio de Industrias y Productividad (MIPRO), en la ciudad de Ambato, Acuerdo Ministerial No. 09432 con fecha del 25 de noviembre de 2009, después de haber cumplido con todos los requisitos legales para la adjudicación de la Personería Jurídica.

REFICH se constituye como una organización de segundo piso que apoya, coordina y ejecuta procesos alternativos de intermediación financiera con Estructuras Financieras Populares y Locales en la provincia de Chimborazo, que fomenta la unión, responsabilidad, confianza y la solidaridad de sus 18 Filiales ubicada en los cantones: Alausí, Pallatanga, Colta, Guamote, Riobamba, Chambo, Guano y Chunchi.

La ciudad de Riobamba el 11 y 12 de diciembre del año 2009, se constituyó en el escenario de encuentro y discusión de los diferentes representantes de Cajas, Bancos y Grupos Solidarios del país, en donde discutieron y analizaron la propuesta del Proyecto de Ley del Sistema Financiero Popular y Solidario, ante la desigual participación de este tipo de organizaciones locales dentro de las estructuras legales; para crear los espacios y la oportunidad de que este sector exponga sus experiencias, necesidades y presenten alternativas válidas para la construcción de un frente activo que permita incorporar sus realidades a la discusión de dicho proyecto de Ley.

Considerada por sus Filiales como un espacio democrático de integración y cooperación mutua entre cooperativas, cajas de ahorro y crédito y grupos asociativos, creada para fortalecer el trabajo de las Estructuras Financieras Locales filiales que son actores indiscutibles de la Economía Popular y Solidaria, a través de la capacitación, asistencia técnica y asesoramiento, comprometidos con el Desarrollo Económico Local de las comunidades, parroquias y cantones a los que pertenecen.

MISION:

La Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo es una organización integradora conformada por Estructuras Financieras Locales que tienen objetivos comunes y basa su trabajo en principios y valores, articulando servicios financieros y no financieros entre sus filiales, impulsando el desarrollo socio-económico de la provincia con representatividad local e incidencia nacional.

VISION:

Al 2013 la Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo es una organización ética, social y financieramente sostenible que promueve el desarrollo socio económico de los territorios rurales y urbano marginales de la provincia brindando servicios financieros y no financieros de calidad que responden a las necesidades y oportunidad de sus filiales.

ROLES Y FUNCIONES

- ✓ Promover el acceso a fondos de operación para dinamizar los productos financieros
- ✓ Fortalecer el desempeño social, financiero y administrativo
- ✓ Representar e incidir políticamente en los espacios públicos y privados para la toma de decisiones a favor del sector
- ✓ Orientar los servicios financieros y no financieros al desarrollo de la Economía Popular y Solidaria
- ✓ Garantizar la equidad e igualdad en el acceso a derechos y beneficios de las filiales dentro de la Red

✓ Certificar el desempeño de balance social y financiero.

✓ Crear agendas de cooperación y alianzas institucionales con el sector público y privado.

1. Representatividad y Asociatividad (Gobierno de la Red)

✓ Mejorar representatividad de sus filiales dentro de la estructura del directorio de REFICH, para garantizar la participación equitativa en la toma de decisiones.

✓ Afianzar las relaciones de las filiales para garantizar el empoderamiento y compromiso en la gestión socio organizativo de la REFICH.

2. Fortalecimiento Institucional y Asistencia Técnica (Desempeño y sostenibilidad del Sistema)

✓ Fortalecer permanente los canales de comunicación.

✓ Ejecutar programas validados de capacitación y fortalecimiento del sistema.

✓ Brindar servicios profesionales propios que respondan a las necesidades reales de las filiales.

✓ Contar con una estructura organizada que nos permita generar economías de escala por medio de la asistencia técnica.

✓ Estructurar herramientas de evaluación y seguimiento que nos permita brindar servicios de validación y certificación de la experiencia financiera y social de las filiales.

3. Articulación de procesos (cadenas productivas, políticas, financieras y sociales)

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN
ENERO 2012 – DICIEMBRE 2012
ABREVIATURAS

ABREVIATURA	SIGNIFICADO
JLMG	Jose Luis Morales Garcés
MLVR	María Lorena Valle Romero
AP	Archivo Permanente
AC	Archivo Corriente
HM	Hoja de Marcas
AB	Abreviaturas
PADG	Programa de Auditoría
SA	Solicitud de Autorización
EDE	Entrevista al Director Ejecutivo de la entidad.
PAI	Plan de Auditoría Informática
ECM	Entrevista a la encargada del Departamento C.M
PCI	Programa de Control Interno
CCI	Cuestionario de Control Interno
PE	Principios de la Entidad
LC	Legajo Corriente
PAE	Programa de Auditoría de Ejecución
HH	Hoja de Hallazgos
MR	Matriz de Resultados
MP	Memorándum de Planeación

ELABORADO POR:	J.M	**FECHA:**	17-03-2014
REVISADO POR:	M.V	**FECHA:**	20-03-2014

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

ENERO 2012 – DICIEMBRE 2014

HOJA DE MARCAS

MARCA	SIGNIFICADO
¥	Confrontado con libros
§	Cotejado con documento
µ	Corrección realizada
¢	Comparado en auxiliar
¶	Hallazgo (Observación)
©	Confrontado correcto
^	Sumas verificadas
✓	Cumple con requisitos
Ø	No reúne requisitos
S	Solicitud de confirmación enviada
SI	Solicitud de confirmación recibida inconforme
S	Totalizado
Ã	Conciliado
SC	Solicitud de confirmación recibida conforme
Æ	Circularizado
SIA	Solicitud de confirmación recibida inconforme pero aclarada
Y	Inspeccionado

ELABORADO POR:	J.M	**FECHA:**	**18-03-2014**
REVISADO POR:	M.V	**FECHA:**	**21-03-2014**

4.6.2 Archivo Corriente

MORALES & VALLE
ASOCIADOS
AUDITORES INDEPENSIENTES CIA. LTDA

ARCHIVO
CORRIENTE

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

MARZO 2014 – MAYO 2014

FASE I: DIAGNÓSTICO SITUACIONAL

DIAGNÓSTICO GENERAL DE LA INSTITUCIÓN

INDICE

ELABORADO POR:	J.M	**FECHA:**	18-03-2014
REVISADO POR:	M.V	**FECHA:**	21-03-2014

MORALES & VALLE ASOCIADOS
AUDITORES INDEPENSIENTES CIA. LTDA

PADG

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

PROGRAMA DE AUDITORÍÁ- DIAGNÓSTICO GENERAL

N°	DESCRIPCIÓN	REF P/T	REALIZADO POR:	FECHA
	OBJETIVOS:			
1	Obtener la información y recursos necesarios para poder ejecutar la Auditoria Informática de la Seguridad de la Información.			
2	Establecer las normas o leyes a las que esta sujetas a cumplir la Entidad.			
3	Establecer la Estructura Orgánica que posee la Entidad.			
	PROCEDIMIENTOS:			
1	Solicitar al Director Ejecutivo de la entidad que nos proporcione la información y recursos necesarios para poder realizar el trabajo de Auditoria.	SA	JLMG	**09-04-2014**
2	Entrevistar al Director Ejecutivo de la entidad.	EDE $^{1}/_{3}$ - $^{3}/_{3}$	JLMG	**12-04-2014**
3	Solicitar al Director Ejecutivo, Principios de la entidad.	PE $^{1}/_{2}$ - $^{2}/_{2}$	JLMG	**13-04-2014**
4	Entrevista a la encargada del Departamento de Control y Monitoreo.	ECM $^{1}/_{4}$ - $^{4}/_{4}$	JLMG	**13-04-2014**

ELABORADO POR:	J.M	**FECHA:**	**06-04-2014**
REVISADO POR:	M.V	**FECHA:**	**09-04-2014**

MORALES & VALLE
ASOCIADOS
AUDITORES INDEPENSIENTES CIA. LTDA

SA

Riobamba, 09 de Marzo del 2014

Ing. Edwin Niamiña Lara
DIRECTOR EJECUTIVO DE LA RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO.
Presente.

De mi consideración:

En vista a la autorización que se me ha concedido anteriormente para la realización de una Auditoría Informática a la Seguridad Información para medir el grado de cumplimiento que la Entidad tiene sobre las tecnologías de información, basada en las normas y reglamentos emitidos Organización Internacional de Estandarización (I.S.O) del grupo 17799, me dirijo a Ud. para solicitarle de la manera más comedida su completa colaboración por parte del personal de la Entidad, para acceder a la documentación e información necesaria con la finalidad de poder llevar a cabo la presente investigación solicitada.

Por la atención a la presente reitero mis más sinceros agradecimientos.

Atentamente,

Ma. Lorena Valle Romero
SUPERVISOR

ELABORADO POR:	J.M	**FECHA:**	**09-04-2014**
REVISADO POR:	M.V	**FECHA:**	**11-04-2014**

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

AUTORIDAD DE LA ENTIDAD

ENTREVISTA – Ing. Edwin Niamiña

OBJETIVO: Conocer las instalaciones, actividades y situación actuales de la Entidad, así como del conocimiento que tiene como autoridad REFICH.

1. **RAZÓN SOCIAL**: Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo. (REFICH).
2. **FECHA DE CRACION DE LA INSTITUCIÓN:** Noviembre de 2009 mediante Acuerdo Ministerial
3. **DIRECCIÓN:** Calle Río Chanchan 18-33 entre Chile y Villarroel.
4. **PROVINCIA:** Chimborazo.
5. **CANTÓN:** Riobamba.
6. **PARROQUIA:** Lizarzaburo
7. **HORARIO DE ATENCIÓN:**

   8:30 am - 12:30 am

   13:30am - 17:30 am

8. - **TELÉFONOS:** 032941-459
9. **AUTORIDADES:**

Presidenta: Ing. Carmen Cecilia Uvidia

Director Ejecutivo: Ing. Edwin Ñamiña Lara

ELABORADO POR:	J.M	**FECHA:**	**13-04-2014**
REVISADO POR:	M.V	**FECHA:**	**16-04-2014**

10. FUNCIONES Y ATRUBUCIONES: Soy el representante legal de la Entidad, en tal sentido mis funciones y atribuciones se sujetaran a lo dispuesto en las leyes y reglamentos vigentes.

11. NÚMERO DE PERSONAS EN LA ENTIDAD: La Entidad posee 5 personas distribuidos en el departamento de Contabilidad, Fortalecimiento Técnico, Control y Monitoreo y Dirección Ejecutiva.

12. CUENTA CON ESPACIO PROPIO EL DEPARTAMENTO DE CONTROL Y MONITOREO: Al momento el departamento cuenta con su propio Espacio para el trabajo diario de control y monitoreo.

PREGUNTAS CERRADAS

1. ¿El presupuesto asignado a la Entidad por parte de la Asamblea de Socios es adecuado?

SI: X

NO:

2. ¿El porcentaje que la Entidad destina al departamento cubre con las necesidades?

SI:

NO: X

3. ¿El número de encargados del departamento es adecuado?

SI: X

NO:

ELABORADO POR:	J.M	**FECHA:**	13-04-2014
REVISADO POR:	M.V	**FECHA:**	16-04-2014

4. ¿Existe alguna persona responsable del departamento de control y monitoreo?

SI: X

NO:

5. ¿Anteriormente se han realizado Auditorías Informáticas a la seguridad de la información de la Entidad?

SI:

NO: X

6. *¿Cuenta la Entidad con un manual de funciones*?

SI:

NO: X

GRACIAS POR LA ATENCIÓN

ELABORADO POR:	J.M.	**FECHA:**	**13-04-2013**
REVISADO POR:	M.V	**FECHA:**	**16-04-2013**

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

PRINCIPIOS DE LA ENTIDAD

PRINCIPIOS

A más de lo principios establecidos por la Ley de Economía Popular y Solidaria.

- Integrará y fortalecerá las Estructuras de Finanzas Populares y Solidarias de la provincia de Chimborazo para impulsar el desarrollo socio-económico local y solidario, en el sector rural, urbano marginal y urbano de la provincia de Chimborazo.
- Fomentara a través de sus filiales el fortalecimiento de las microempresas existentes y fomentar la creación de otras que permitan elevar el nivel de vida de cada una de las localidades.
- Posicionara a la Red como una organización de Finanzas Populares que incida política, social y económicamente en los acontecimientos de trascendental importancia en la provincia.
- Promoverá la integración con entidades fraternas nacionales y extranjeras en procura de fortalecer el desarrollo institucional y del sistema cooperativo.

GESTIÓN INSTITUCIONAL

Considerada por sus Filiales como un espacio democrático de integración y cooperación mutua entre cooperativas, cajas de ahorro y crédito y grupos asociativos, creada para fortalecer el trabajo de las Estructuras Financieras Locales filiales que son actores indiscutibles de la Economía Popular y Solidaria, a través de la capacitación, asistencia técnica y asesoramiento, comprometidos con el Desarrollo Económico Local de las comunidades, parroquias y cantones a los que pertenecen.

ELABORADO POR:	J.M	**FECHA:**	**13-04-2014**
REVISADO POR:	M.V	**FECHA:**	**16-04-2014**

ESTRUCTURA ORGANIZATIVA

La Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo parte de la premisa organizativa basada en el desarrollo eficiente, armónico y democrático expresado en su organigrama y manuales de procedimientos.

ORGANIGRAMAS

La Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo parte de la premisa organizativa basada en el desarrollo eficiente, armónico y democrático expresado y concretado en los ORGANIGRAMAS ESTRUCTURAL, conforme las funciones que cumplen cada uno de su personal.

ELABORADO POR:	J.M	**FECHA:**	**13-04-2014**
REVISADO POR:	M.V	**FECHA:**	**16-04-2014**

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO
AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

DEPARTAMENTO DE CONTROL Y MONITOREO

ENTREVISTA – Ing. Lorena Moreno

OBJETIVO: Conocer las instalaciones, actividades y situación en el área informática de la Institución.

1. ¿Cuántos computadores tiene el departamento de Control y Monitoreo de la REFICH?

El departamento cuenta con 1 computador para el trabajo de control y monitoreo.

2. ¿Cuál es el número de encargados del departamento?

En el departamento existen 2 encargados del control y monitoreo.

3. ¿El lugar donde se encuentra ubicado el departamento está seguro de inundaciones, robos o cualquier otra situación que ponga en peligro los equipos informáticos?

Si ya que contamos con un adecuado sistema de seguridad contra incendios.

PREGUNTAS CERRADAS

1. ¿Cree usted que la infraestructura física es adecuada?

SI ☐ ***NO*** [X]

2. ¿El mobiliario abastece para el trabajo realizado en el departamento?

SI ☐ ***NO*** [X]

ELABORADO POR:	J.M	**FECHA:**	13-04-2014
REVISADO POR:	M.V	**FECHA:**	16-04-2014

3. ¿Se aplica normas de control interno al manejo de la información del departamento?

SI [ ] ***NO*** [x]

4. ¿Se realiza mantenimiento preventivo a los equipos informáticos?

SI [ ] ***NO*** [x]

5. ¿Se realiza mantenimiento correctivo a los equipos informáticos?

SI [x] ***NO*** [ ]

6. ¿Cuenta con contraseñas para el manejo de la información?

SI [x] ***NO*** [ ]

7. ¿Cuenta con designación de responsabilidades para el cuidado de la información dentro del departamento?

SI [ ] ***NO*** [x]

8. ¿Cuenta con personal de experiencia?

SI [x] ***NO*** [ ]

9. ¿El departamento cuenta con un plan de capacitación para el personal?

SI [ ] ***NO*** [x]

ELABORADO POR:	J.M	**FECHA:**	13-03-2014
REVISADO POR:	M.V	**FECHA:**	16-03-2014

10. ***¿Cuentan con licencias del software utilizados para el control y monitoreo que realiza el departamento?***

SI [X] ***NO*** [ ]

GRACIAS POR LA ATENCIÓN

ELABORADO POR:	J.M	**FECHA:**	**13-04-2014**
REVISADO POR:	M.V	**FECHA:**	**16-04-2014**

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

MARZO 2014 – MAYO 2014

FASE II – CONTROL INTERNO

EVALUACIÓN CONTROL INTERNO

INDICE

ELABORADO POR:	J.M	**FECHA:**	**18-04-2014**
REVISADO POR:	M.V	**FECHA:**	**21-04-2014**

MEMORÁNDUM DE PLANEACIÓN

1. DATOS DE LA ENTIDAD

Razón Social: Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo

Provincia: Chimborazo

Cantón: Riobamba

Parroquia: Lizarzaburo

Dirección: Río Chanchan 18-33 entre Chile y Villarroel

Teléfonos: 032941-459

Ubicación Geográfica: Riobamba - Ecuador

2. PROGRAMA

Programa de Auditoría: Auditoría Informática de la Seguridad de la información.

Documento de Autorización: Orden de Trabajo N° 001

Períodos de la Auditoría: Enero 2012 – Diciembre 2012

ELABORADO POR:	J.M	**FECHA:**	**19-04-2014**
REVISADO POR:	M.V	**FECHA:**	**21-04-2014**

3. OBJETIVO DEL EXAMEN

Realizar una Auditoría Informática de la Seguridad de la Información en la Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo "REFICH" de la provincia de Chimborazo, cantón Riobamba, período 2012, para medir el grado de cumplimiento de las normas de control interno.

4. ALCANCE DEL EXAMEN

La Auditoría Informática de la Seguridad de la Información, es la revisión y la evaluación de los controles internos, sistemas, procedimientos y equipos informáticos, su eficiencia y seguridad, de la organización de los procesamientos de la información, con la finalidad de lograr una utilización más eficiente y segura, que servirá para una adecuada toma de decisiones dentro del departamento y la Entidad.

5. ACTIVIDADES INSTITUCIONALES

- Análisis financieros.
- Fortalecimientos Técnicos mediante indicadores.
- Contabilidad.
- Capacitaciones y Actualizaciones del medio.
- Soporte Técnico y aplicaciones de sistemas informáticos.

ELABORADO POR:	J.M	**FECHA:**	19-04-2014
REVISADO POR:	M.V	**FECHA:**	21-04-2014

6. NORMATIVIDAD APLICABLE

- La Ley Orgánica de Economía Popular y Solidaria.
- Organización Internacional de Estandarización (ISO) 17799 aplicada a la Seguridad de la Información.

7. IDENTIFICACIÓN DE ÁREAS CRÍTICAS

La presente acción de control está orientada al Departamento de Control y Monitoreo, para verificar el proceso técnico de la información de la entidad.

- **Evaluación de sistemas de la Entidad.-** El sistemas debe ser evaluada detalladamente, para lo cual se debe revisar si existen realmente sistemas entrelazados como un todo o un bien si existen programas aislados y si existe un plan estratégico para la elaboración de sistemas informático.
- **Evaluación del análisis.-** Evaluar las políticas, procedimientos y las normas que se tienen para llevar a cabo el análisis.
- **Evaluación del diseño lógico del sistema de la Entidad.-** Al tener el análisis del diseño lógico del sistema, se comprobara lo que realmente se está obteniendo, donde se evaluara lo planeado, como fue planeado y lo que se está obteniendo.

ELABORADO POR:	J.M	**FECHA:**	**19-04-2014**
REVISADO POR:	M.V	**FECHA:**	**21-04-2014**

➢ **Evaluación del desarrollo del sistema de la Entidad.- S**e auditara los programas, diseño, lenguaje utilizado, interconexión entre los programas y características del hardware utilizado para el desarrollo del sistema.

8. PERSONAL DE LA ENTIDAD

AUTORIDADES:

Presidenta: Ing. Carmen Cecilia Uvidia

Director Ejecutivo: Ing. Edwin Ñamiña Lara

PERSONAL DE CONTROL Y MONITOREO:

Técnico 1: Ing. María Lorena Moreno

Técnico 2: Ing. Olger Sarango Lapo

PERSONAL CONTABLE:

Contadora: Ing. Mayra Sánchez

PERSONAL DE FORTALECIMIENTO TÉCNICO

Fortalecimiento: Ing. Gabriela Ramos

9. PERSONAL DE AUDITORÍA

➢ **AUDITOR:** Jose Luis Morales Garcés

ELABORADO POR:	J.M	**FECHA:**	**19-04-2014**
REVISADO POR:	M.V	**FECHA:**	**21-04-2014**

- **SUPERVISOR:** María Lorena Valle Romero

10. INFORMES A EMITIR Y FECHAS DE ENTREGA

El informe de auditoría se emitirá dentro de los 120 días de iniciado el proceso, el primer informe se lo entregara a la Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo, el segundo informe a la Escuela Superior Politécnica de Chimborazo y el tercer informe a la Facultad de Administración de Empresas.

11. PRESUPUESTO DE TIEMPO

ACTIVIDADES	TIEMPO (DIAS)	TOTAL (H/M)
Planificación de Auditoría	21	504
Ejecución de la Auditoría	45	1080
Evaluación de Descargos	30	720
Redacción del Informe Administrativo	15	360
Redacción del Informe de Auditoria	9	216
TOTAL	120	2880

ELABORADO POR:	J.M	**FECHA:**	**19-04-2014**
REVISADO POR:	M.V	**FECHA:**	**21-04-2014**

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

PROGRAMA DE AUDITORÍA – EVALUACIÓN DEL CONTROL INTERNO

N°	DESCRIPCIÓN	REF P/T	REALIZADO POR:	FECHA
	OBJETIVOS:			
1	Verificar el cumplimiento de las normas ISO/IEC 17799 sobre el uso de las Seguridad de la Información sujetas a cumplir la Entidad.			
2	Establecer la colaboración del personal de la entidad a fin de obtener información y conocimientos sobre las actividades que esta mantiene.			
3	Determinar la matriz de resultados para asegurar el manejo correcto de los recursos.			
4	Determinar los aspectos críticos a través de la elaboración de hojas de hallazgos con sus conclusiones y recomendaciones respectivas.			
	PROCEDIMIENTOS:			
1	Elaboración del Plan de Auditoría de Control I.	EP	JLMG	02-05-2014
2	Aplicar Cuestionarios de Control Interno			
2.1	Política de Seguridad	CCI 1/9	JLMG	03-05-2014
2.2	Organización de Seguridad	CCI 2/9	JLMG	03-05-2014
2.3	Clasificación y control de Activos	CCI 3/9	JLMG	06-05-2014

ELABORADO POR:	J.M	**FECHA:**	23-05-2014
REVISADO POR:	M.V	**FECHA:**	24-05-2014

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

PROGRAMA DE AUDITORÍA – EVALUACIÓN DEL CONTROL INTERNO

N°	DESCRIPCIÓN	REF P/T	REALIZADO POR:	FECHA
2.4	Seguridad del Personal	CCI 4/9	JLMG	06-05-2014
2.5	Seguridad física y del entorno	CCI 5/9	JLMG	07-05-2014
2.6	Comunicación/ administración de operaciones	CCI 6/9	JLMG	07-05-2014
2.7	Control de acceso	CCI 7/9	JLMG	08-05-2014
2.8	Desarrollo y mantenimiento del sistema	CCI 8/9	JLMG	08-05-2014
2.9	Plan de continuidad empresarial.	CCI 9/9	JLMG	09-05-2014
3	Evaluación de Riesgo			
3.1	Tabulación y Ponderación de Riesgo	CCI1/9-9/9	JLMG	15-05-2014
4	Elaboración de la Matriz de Resultados	MR	JLMG	20-05-2014

ELABORADO POR:	J.M	**FECHA:**	23-05-2014
REVISADO POR:	M.V	**FECHA:**	23-05-2014

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

PLAN DE AUDITORÍA DE CONTROL INTERNO

1. MOTIVO DE LA EVALUACIÓN DEL CONTROL INTERNO.- Esta evaluación del Control Interno está relacionada con las normas ISO 17799, de conformidad con orden de trabajo Nº 001 para su ejecución.

2. OBJETIVOS DE LA EVALUACIÓN DE CONTROL INTERNO.- Determinar si el Control Interno proporciona seguridad razonable en cuanto a la obtención de objetivos y que estén relacionados con la eficiencia, eficacia de la gestión y cumplimiento de las disposiciones legales vigentes.

3. ALCANCE DE EVALUACIÓN DE CONTROL INTERNO.- La Evaluación del Control Interno está relacionada con el cumplimiento de la normativa ISO 17799 sobre la Seguridad de la Información, del periodo 2012.

4. AUTORIZACIÓN Y COLABORACIÓN DE LA INSTITUCIÓN.- La autorización y colaboración de la Entidad se la realizará a través de las autoridades y supervisor del Departamento Control y Monitoreo.

5.- EQUIPO DE TRABAJO ENCARGADO DEL LA EVALUACIÓN

- ✓ **SUPERVISOR**: María Lorena Valle Romero
- ✓ **AUDITOR**: Jose Luis Morales Garcés.

ELABORADO POR:	J.M	**FECHA:**	**02-05-2014**
REVISADO POR:	M.V	**FECHA:**	**03-05-2014**

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

CUESTIONARIO DE CI. – POLÍTICA DE SEGURIDAD

N°	DESCRIPCIÓN	RESP. Y CALIF.			OBSERVACIÓN
		SI	NO	N/A	
1	¿El servicio web que dispone el Departamento de monitoreo se adapta a las necesidades de la entidad?	10			
2	¿Las Políticas de Seguridad se encuentran actualizadas?		10		¶Las políticas de seguridad no se encuentra actualizadas.
3	¿Se encuentra programada la ejecución automática del Antivirus en los computadores de los usuarios?		10		¶Existen Computadores infectados en la entidad.
4	¿El software que se mantiene actualmente cumple con las exigencias de los usuarios?	10			
5	¿Posee un perfil de privilegios limitados en el computador?		10		¶Los usuarios poseen un perfil de administrador, por lo tanto su perfil no es limitado.

$$\textbf{Confianza} = \frac{CT}{PT} x100 = \frac{30}{50} x100 = \textbf{60\% Riesgo} = 100 - \text{Confianza} = 100 - 60{,}00 = \textbf{40\%}$$

		NIVEL DE RIESGO		
		BAJO (05-24)	MEDIO (25-49)	ALTO (50-85)
NIVEL DE CONFIANZA	ALTO (76-100)			
	MEDIO (51-75)		✓	
	BAJO (15-50)			

ELABORADO POR:	J.M	**FECHA:**	03-05-2014
REVISADO POR:	M.V	**FECHA:**	03-05-2014

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

CUESTIONARIO DE C.I. – ORGANIZACIÓN DE SEGURIDAD

N°	DESCRIPCIÓN	RESP. Y CALIF.			OBSERVACIÓN
		SI	NO	N/A	
1	¿Se cuanta con un profesional quien de soporte técnico y mantenimiento a los equipos informáticos?	10			
2	¿Se cuenta con un profesional encargado de la seguridad de la información?	10			
4	¿Está determinada las funciones y responsabilidades del profesional encargado de la seguridad de la información?		10		¶No se encuentra determinada las funciones y responsabilidades del encargado de la seguridad de la información.
5	¿El área informática de la Institución mantiene una segregación adecuada de funciones?	10			
6	¿La determinación de funciones y responsabilidades garantizarán una adecuada segregación para así evita la existencia de funciones incompatibles?	10			

$$\textbf{Confianza} = \frac{CT}{PT} x\ 100 = \frac{10}{50} x\ 100 = \textbf{20\%} \quad \textbf{Riesgo} = 100 - \text{Confianza} = 100 - 20 = \textbf{80\%}$$

		NIVEL DE RIESGO		
		BAJO (05-24)	MEDIO (25-49)	ALTO (50-85)
NIVEL DE CONFIANZA	ALTO (76-100)	✓		
	MEDIO (51-75)			
	BAJO (15-50)			

ELABORADO POR:	J.M	**FECHA:**	03-05-2014
REVISADO POR:	M.V	**FECHA:**	03-05-2014

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

CUESTIONARIO DE C.I. – CLASIFICACIÓN Y CONTROL DE ACTIVOS

N°	DESCRIPCIÓN	RESP. Y CALIF.			OBSERVACIÓN
		SI	NO	N/A	
1	¿Se tiene un inventario de activos claramente identificado?	10			
2	¿Se sabe quiénes son los usuarios de los activos identificados?	10			
3	¿Se tiene asignado un responsable de los activos que tiene la entidad identificada?	10			
4	¿Existen políticas y procedimientos para la clasificación y etiquetado de los activos?		10		¶No existe políticas y procedimientos de clasificación y etiquetado en los activos.
5	¿Existe un criterio para valorar o clasificar los activos de la entidad?	10			

$$\textbf{Confianza} = \frac{CT}{PT} x\ 100 = \frac{10}{50} x\ 100 = \textbf{20\%} \quad \textbf{Riesgo} = 100 - \text{Confianza} = 100 - 20 = \textbf{80\%}$$

		NIVEL DE RIESGO		
		BAJO (05-24)	MEDIO (25-49)	ALTO (50-85)
NIVEL DE CONFIANZA	ALTO (76-100)	✓		
	MEDIO (51-75)			
	BAJO (15-50)			

ELABORADO POR:	J.M	**FECHA:**	06-05-2014
REVISADO POR:	M.V	**FECHA:**	07-05-2014

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

CUESTIONARIOS C.I. – SEGURIDAD DEL PERSONAL

N°	DESCRIPCIÓN	RESP. Y CALIF.			OBSERVACIÓN
		SI	NO	N/A	
1	¿Se tienen definidos roles y responsabilidades de la seguridad de los empleados?	10			
2	¿Se lleva a cabo chequeos de verificación de antecedentes de los empleados?	10			
3	¿Existe un proceso disciplinario en casos de violaciones a las políticas de seguridad?		10		¶No existe una política de seguridad para sancionar a los empleados.
4	¿Los empleados de la entidad reciben el apropiado conocimiento, capacitación y actualizaciones?	10			
5	¿Los empleados firman acuerdos de confidencialidad o no revelación juntos a los términos y condiciones del contrato del empleado?		10		¶No existen acuerdos de confidencialidad o no revelación en los contratos a los empleados.

$$\textbf{Confianza} = \frac{CT}{PT} x\ 100 = \frac{20}{50} x\ 100 = \textbf{40\%} \quad \textbf{Riesgo} = 100 - \text{Confianza} = 100 - 40 = \textbf{60\%}$$

		NIVEL DE RIESGO		
		BAJO (05-24)	MEDIO (25-49)	ALTO (50-85)
NIVEL DE CONFIANZA	ALTO (76-100)			
	MEDIO (51-75)		✓	
	BAJO (15-50)			

ELABORADO POR:	J.M	**FECHA:**	06-05-2014
REVISADO POR:	M.V	**FECHA:**	07-05-2014

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

CUESTIONARIO C.I. - SEGURIDAD FÍSICA Y DEL ENTORNO

N°	DESCRIPCIÓN	RESP. Y CALIF.			OBSERVACIÓN
		SI	NO	N/A	
1	¿Existe un plan de mantenimiento para los equipos de la entidad?		10		¶No existe un cronograma de actividades para el mantenimiento de equipos.
2	¿Los equipos se encuentran protegidos al contacto con los usuarios?		10		¶ No se encuentran los equipos protegidos al contacto de los usuarios.
3	¿Aplican procedimientos de eliminación de equipos o reutilización de los mismos?		10		¶No existe procedimientos para la eliminación de equipos o reutilización.
4	¿El cableado de energía eléctrica está protegido para evitar daños?	10			
5	¿Existe un criterio para el manejo de la seguridad de los equipos que se encuentren fuera de la entidad?	10			

$$\textbf{Confianza} = \frac{CT}{PT} x\ 100 = \frac{30}{50} x\ 100 = \textbf{60\%} \quad \textbf{Riesgo} = 100 - \text{Confianza} = 100 - 60 = \textbf{40\%}$$

		NIVEL DE RIESGO		
		BAJO (05-24)	MEDIO (25-49)	ALTO (50-85)
NIVEL DE CONFIANZA	ALTO (76-100)			
	MEDIO (51-75)		✓	
	BAJO (15-50)			

ELABORADO POR:	J.M	**FECHA:**	07-05-2014
REVISADO POR:	M.V	**FECHA:**	08-05-2014

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

CUESTIONARIO C.I. – COMUNICACIÓN/ ADMINISTRACIÓN DE OPERACIONES

N°	DESCRIPCIÓN	RESP. Y CALIF.			OBSERVACIÓN
		SI	NO	N/A	
1	¿Se realizan respaldos diarios de la información y software?		10		¶No se realizan respaldos de la base de datos.
2	¿Existe segregación de funciones para modificaciones del sistema?	10			
3	¿Existe un procedimiento para la gestión de cambio de los servicios que se tiene en la entidad?	10			
4	¿Existe criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas?		10		¶No existen criterios de aceptación para los sistemas de información, actualizaciones y versiones nuevas.
5	¿Se tiene un registro de actividades realizadas por el operador de monitoreo?	10			

$$\textbf{Confianza} = \frac{CT}{PT} x\ 100 = \frac{20}{50} x\ 100 = \textbf{40\%} \quad \textbf{Riesgo} = 100 - \text{Confianza} = 100 - 40 = \textbf{60\%}$$

		NIVEL DE RIESGO		
		BAJO (05-24)	MEDIO (25-49)	ALTO (50-85)
NIVEL DE CONFIANZA	ALTO (76-100)			
	MEDIO (51-75)		✓	
	BAJO (15-50)			

ELABORADO POR:	J.M	**FECHA:**	07-05-2014
REVISADO POR:	M.V	**FECHA:**	08-05-2014

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

CUESTIONARIO C.I. – CONTROL DE ACCESOS

N°	DESCRIPCIÓN	RESP. Y CALIF.			OBSERVACIÓN
		SI	NO	N/A	
1	¿Existe un administrador que controle a los usuarios?	10			.
2	¿Se obliga cada cierto tiempo a cambiar la contraseña automática?	10			
3	¿Existe un procedimiento formal de entrega/ recepción de las claves de usuario?		10		¶No existe un procedimiento formal de entrega/ recepción de claves para los usuarios.
4	¿Se restringe y controla el uso de programas no aplicables para la entidad?	10			
5	¿Se tiene un único registro de identificación y autentificación de usuarios para el acceso al sistema?	10			

$$\textbf{Confianza} = \frac{CT}{PT}\ x\ 100 = \frac{10}{50}\ x\ 100 = \textbf{20\%} \quad \textbf{Riesgo} = 100 - \text{Confianza} = 100 - 20 = \textbf{80\%}$$

		NIVEL DE RIESGO		
		BAJO (05-24)	MEDIO (25-49)	ALTO (50-85)
NIVEL DE CONFIANZA	ALTO (76-100)	✓		
	MEDIO (51-75)			
	BAJO (15-50)			

ELABORADO POR:	J.M	**FECHA:**	08-05-2014
REVISADO POR:	M.V	**FECHA:**	09-05-2014

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

CUESTIONARIO C.I.- DESARROLLO Y MANTENIMIENTO DEL SISTEMA

N°	DESCRIPCIÓN	RESP. Y CALIF.			OBSERVACIÓN
		SI	NO	N/A	
1	¿El personal informa si ha observado alguna debilidad, sospecha de debilidad o violación de las seguridades de los sistemas?	10			.
2	¿Existe un encargado de los procedimientos de gestión para el control de manera rápida y efectiva de los incidentes reportados?	10			
3	¿Existe un procedimiento formal que asegure el reporte al Director Ejecutivo?		10		¶No existe un procedimiento formal que asegure el reporte al Director Ejecutivo.
4	¿Existe un mecanismo para monitorear y cuantificar los incidentes reportados?	10			
5	¿Se tiene reporte de los estados de los incidentes atendidos?	10			

$$\textbf{Confianza} = \frac{CT}{PT} x\ 100 = \frac{10}{50} x\ 100 = \mathbf{20\%} \quad \textbf{Riesgo} = 100 - \text{Confianza} = 100 - 20 = \mathbf{80\%}$$

		NIVEL DE RIESGO		
		BAJO (05-24)	MEDIO (25-49)	ALTO (50-85)
NIVEL DE CONFIANZA	ALTO (76-100)	✓		
	MEDIO (51-75)			
	BAJO (15-50)			

ELABORADO POR:	J.M	**FECHA:**	08-05-2014
REVISADO POR:	M.V	**FECHA:**	09-05-2014

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

CUESTIONARIO C.I. - PLAN DE LA CONTINUIDAD COMERCIAL

N°	DESCRIPCIÓN	RESP. Y CALIF.			OBSERVACIÓN
		SI	NO	N/A	
1	¿Se tiene un plan de continuidad del negocio o contingencia acorde a los objetivos de la entidad?	10			.
2	¿El plan se encuentra difundido formalmente en la entidad?	10			
3	¿El plan de continuidad de negocio es revisado periódicamente por la alta gerencia?	10			
4	¿Están definidos formalmente los procedimientos manuales de los procesos claves que se podrían en ejecución en caso de una contingencia?		10		¶No existen procedimientos manuales de los procesos claves para la continuidad del negocio.
5	¿Se realizado pruebas de eficacia al plan de continuidad de negocio?	10			

		NIVEL DE RIESGO		
		BAJO (05-24)	MEDIO (25-49)	ALTO (50-85)
NIVEL DE CONFIANZA	ALTO (76-100)	✓		
	MEDIO (51-75)			
	BAJO (15-50)			

$$\textbf{Confianza} = \frac{CT}{PT} x\ 100 = \frac{10}{50} x\ 100 = \mathbf{20\%} \quad \textbf{Riesgo} = 100 - \text{Confianza} = 100 - 20 = \mathbf{80\%}$$

ELABORADO POR:	J.M	**FECHA:**	09-05-2014
REVISADO POR:	M.V	**FECHA:**	10-05-2014

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO
AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN
MATRIZ DE RESULTADOS DEL CONTROL INTERNO

TABLA N° 19 MATRIZ DE RESULTADOS DEL CONTROL INTERNO

N°	CRITERIO	CAUSA	IMPACTO	NORMA RELACIONDADA
1	Política de Seguridad actualizada	La política de seguridad no se encuentra actualizada	En el documento de Políticas de Seguridad se menciona el Software "Norton Antivirus", sin embargo, éste no es el sistema Antivirus que posee la empresa, lo cual podría afectar a la aplicación de la política de seguridad referente a la protección de equipos a través del antivirus "NOD32" que es el que realmente tiene implementado.	ISO/IEC 17799-1
2	Escaneo automático de Virus en el computador del usuario, los viernes a las 17h00	No se encuentra programada la ejecución automática del Antivirus en los computadores de los usuarios.	Computadores infectados lo cual puede afectar a la disponibilidad del equipo, provocando interrupciones en el trabajo del usuario e incluso pérdida de información afectando la integridad de la información.	ISO/IEC 17799-1
3	Cualquier software a instalarse deberá ser realizado por el departamento de sistemas, el cual se asegurará que provenga de fuentes conocidas y seguras, además de cerciorarse de que dicha instalación no cree conflicto alguno.	Los usuarios tienen perfil "Administrador" en el computador por lo cual pueden instalar cualquier tipo de software.	Afectar al rendimiento del computador del usuario así como también se pueden producir filtraciones de código malicioso de software no autorizado que pueden poner en riesgo la disponibilidad e integridad de la información, además del riesgo legal asociado al tener instalado software sin licencias autorizadas que puede crear demandas o problemas legales entre la institución y los propietarios de software.	ISO/IEC 17799-1
4	Tener definidas las funciones y responsabilidades de Seguridad.	No se encuentran definidas las funciones y responsabilidades de la Seguridad. El cargo ha sido asignado al Auditor Interno en lo referente a la custodia de las claves de los servidores y base de datos principal, transportación de los respaldos a una ubicación externa, revisión de los logs de auditoría y accesos otorgados a los	Que los temas relacionados a la Seguridad de la Información no sean tratados con la debida diligencia, compromiso y de manera efectiva. La Administración de Usuarios está siendo manejada por el Área de Sistemas lo cual puede provocar conflictos de intereses y accesos no autorizados que pueden afectar a la confidencialidad e integridad de la información.	ISO/IEC 17799-2

		usuarios e informe de estas revisiones a la Alta Gerencia.		
5	Política para la clasificación y etiquetado de la información	No existen políticas ni procedimientos para la clasificación y etiquetado de la información.	Accesos no autorizados a la información ya sea esta digital o física, lo cual puede provocar pérdida de la confidencialidad de la información.	ISO/IEC 17799-3
6	Que exista un proceso disciplinario formal para los empleados que han comprometido una vulnerabilidad de seguridad.	No existe un proceso disciplinario en casos de violaciones a las políticas de seguridad por parte de los empleados	Incumplimiento a las políticas de seguridad sin poder sancionar a los responsables.	ISO/IEC 17799-4
7	Firmas de acuerdos confidencialidad o no revelación junto a los términos y condición de los contratos.	Al no establecer en los contratos acuerdos de confidencialidad o no revelación, existe fuga de información por parte de los empleados.	Fuga de información por parte de los empleados de la entidad ya que nos les impide ningún argumento legal para no tomar información valiosa y aplicarla en otra entidad.	ISO/IEC 17799-4
8	Plan de mantenimiento de equipos de usuarios	En el cronograma del Departamento de Sistemas no se evidencian actividades relacionadas al mantenimiento de equipos de los usuarios.	Daños inesperados en los computadores o servidores que pueden afectar a la disponibilidad e integridad de la información y a la continuidad de los procesos normales del negocio.	ISO/IEC 17799-5
9	Los equipos se aíslan o se protegen para reducir los riesgos de las amenazas y peligros medioambientales y para reducir las oportunidades de acceso no Autorizado	Los servidores se encuentran ubicados en un gabinete cerrado dentro del área de Sistemas la cual está separada por paredes falsas de madera, tela y aluminio y contigua a un área de archivos, sin embargo, si cuenta con extintor de incendio, detectores de humo, control de temperatura y humedad, sensores de movimiento, cerradura eléctrica, entre otros.	Fácil propagación del calor en caso de un siniestro al estar junto a un área en el que se guarda material de fácil combustión, lo cual puede comprometer la disponibilidad de los servicios de TI y la continuidad del negocio.	ISO/IEC 17799-5
10	Los equipos destinados a eliminación o reutilización, que contienen disco, se verifican previamente asegurando que toda la información delicada o el software licenciado se destruyen físicamente, o son sobrescritos de manera segura.	No existe un procedimiento formal de eliminación de equipos y se pudo evidenciar que existen computadores que mantienen el nombre del computador identificado por el área a la que pertenecieron anteriormente, lo que evidencia que no se ha aplicado un procedimiento para la reutilización de los mismos.	Accesos no autorizados a la información con la pérdida de confidencialidad que esto conlleva.	ISO/IEC 17799-5

11	Se deben realizar respaldos de la información comercial y software esencial.	En el procedimiento de Respaldos diarios de la Base de Datos principal se indica que "el Auditor Interno firma la bitácora de respaldos de base de datos para dejar constancia de que le han entregado el respaldo", sin embargo, no existe evidencia de la entrega del respaldo al Auditor Interno. Los respaldos de los usuarios, así como las bases de datos de los aplicativos "satélites" (Nómina, Recursos Humanos, Proveeduría, Activos Fijos, Depósitos a Plazo que utilizan otras bases de datos y que se integran al Sistema principal a través de interfaces) no se almacenan en un lugar externo a la institución.	Que no se pueda garantizar la continuidad de las operaciones en el caso de que suceda un siniestro y no se cuente con el último respaldo tanto de la base de datos Oracle como de las demás aplicaciones en una ubicación externa.	ISO/IEC 17799-6
12	Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas de los sistemas durante su desarrollo y antes de su aceptación.	No se pudo evidenciar la existencia de un plan de pruebas para los cambios que se realizan en los sistemas; existe el "Formulario de Control de Versiones de Software" en el cual solo se menciona que se han realizado las pruebas con el usuario y su aceptación, pero no se indican qué pruebas fueron realizadas.	Modificaciones no autorizadas o mal intencionadas que pueden afectar a la integridad o disponibilidad de la información que se encuentra en las bases de datos.	ISO/IEC 17799-6
13	La asignación de claves se debe controlar a través de un proceso de gestión formal.	No existe un procedimiento formal de entrega/recepción de las claves de usuario.	Se pueden crear accesos no autorizados que afecten a la integridad y confidencialidad de la información.	ISO/IEC 17799-7
14	Asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.	No existe un procedimiento formal que asegure el reporte a la Alta Gerencia de los incidentes que puedan poner en riesgo la seguridad de la información.	Que se produzcan incidentes de seguridad que pueden afectar a la integridad, confidencialidad y disponibilidad de la información.	ISO/IEC 17799-8
15	Se debe mantener un solo	No existe una metodología o marco	Que no se puedan integrar los planes de contingencia	ISO/IEC 17799-9

	marco referencial de planes de continuidad comercial para asegurar que todos los planes sean consistentes y para tratar consistentemente los requerimientos de la seguridad de la información e identificar las pruebas y mantenimiento.	referencial formalmente establecido y aprobado que garantice el proceso de Administración de la Continuidad del Negocio. No existe evidencia de la capacitación realizada en los temas relacionados al BCP, tampoco se detallan las actividades a realizar por cada uno de los responsables pues están descritas de manera general. No están definidos los procedimientos y formularios manuales que se van a utilizar cuando ocurra un evento que ponga en riesgo la continuidad de las operaciones, ni las políticas y procedimientos que van a regir durante la contingencia.	departamentales en el momento de una interrupción del negocio. Que la aplicación del plan no sea efectiva afectando la continuidad del negocio.	

ELABORADO POR:	J.M	**FECHA:**	**20-05-2014**
REVISADO POR:	M.V	**FECHA:**	**22-05-2014**

4.7 Comunicación

MORALES & VALLE ASOCIADOS
AUDITORES INDEPENSIENTES CIA. LTDA

LC

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

ABRIL 2014 – MAYO 2014

FASE III - EJECUCIÓN

DETERMINACIÓN DE HALLAZGOS

INDICE

ELABORADO POR:	J.M	**FECHA:**	03-05-2014
REVISADO POR:	M.V	**FECHA:**	05-05-2014

4.7.1 Programa de Informe final de Auditoría

MORALES & VALLE ASOCIADOS
AUDITORES INDEPENSIENTES CIA. LTDA

PAE

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

PROGRAMA DE AUDITORÍA – DETERMINACIÓN DE HALLAZGOS

N°	DESCRIPCIÓN	REF P/T	REALIZADO POR:	FECHA
	OBJETIVOS:			
1	Determinar los hallazgos con las respectivas conclusiones y recomendaciones para que sean tomados en cuantas por parte de las autoridades para determinar las medidas correctivas en beneficio y mejoramiento del Departamento de Control y Monitoreo.			
	PROCEDIMIENTOS:			
1	Elaboración de Hojas de Hallazgos.	HH $^{1}/_{21}$- $^{21}/_{21}$	JLMG	07-06-2014

ELABORADO POR:	J.M	**FECHA:**	06-06-2014
REVISADO POR:	M.V	**FECHA:**	08-06-2014

4.7.2 Hoja de Hallazgos

MORALES & VALLE ASOCIADOS
AUDITORES INDEPENSIENTES CIA. LTDA

HH 01/22

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO
AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN
HALLAZGOS N° 01
POLÍTICA DE SEGURIDAD NO ACTUALIZADA

Condición.- Las Políticas de Seguridad no se encuentran actualizadas.

Criterio.- Política de Seguridad actualizada.

Causa.- Si las Políticas de Seguridad no se encuentran actualizadas, tendríamos una afectación en los sistemas por parte de los virus informáticos.

Efecto.- En el documento de Políticas de Seguridad se menciona el Software "Norton Antivirus", sin embargo, éste no es el sistema Antivirus que posee la empresa, lo cual podría afectar a la aplicación de la política de seguridad referente a la protección de equipos a través del antivirus "NOD32" que es el que realmente tiene implementado.

Conclusión.- La Política de Seguridad no se encuentra actualizada o no ha sido correctamente revisada.

Recomendación.- El Director Ejecutivo deberá disponer que el Departamento de Control y Monitoreo realice revisiones periódicas a la política de seguridad cada vez que se realicen cambios significativos en la tecnología o en los procedimientos del área de Sistemas así como revisiones que permitan verificar el cumplimiento de la Política de Seguridad debe ser una directriz general para una adecuada administración de la Seguridad de la Información de la entidad.

ELABORADO POR: J.M	**FECHA:** 10-06-2014
REVISADO POR: M.V	**FECHA:** 12-06-2014

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

HALLAZGOS N° 02

EJECUCIÓN AUTOMÁTICA DEL ANTIVIRUS

Condición.- Existen computadores infectados en la entidad.

Criterio.-Escaneo automático de Virus en el computador del usuario, los viernes a las17h00.

Causa.- No se encuentra programada la ejecución automática del Antivirus en los computadores de los usuarios.

Efecto.- Computadores infectados lo cual puede afectar a la disponibilidad del equipo, provocando interrupciones en el trabajo del usuario e incluso pérdida de información afectando la integridad de la información.

Conclusión.- La política no posee el control para que se cumpla la ejecución automática del antivirus en los computadores de los usuarios lo cual denota una falta de control interno que permita verificar el cumplimiento de la Política de Seguridad.

Recomendación.- El Director Ejecutivo deberá disponer al Departamento de Control monitoreo que incluya en su programa anual la revisión periódica del cumplimiento de la política de seguridad verificando la correcta implementación de los controles necesarios para su aplicabilidad.

ELABORADO POR:	J.M	**FECHA:**	**10-06-2014**
REVISADO POR:	M.V	**FECHA:**	**12-06-2014**

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

HALLAZGOS N° 03

CONTROL DE LOS USUARIOS DE PERFIL

Condición.- Los usuarios poseen un perfil de administrador, por lo tanto su perfil no es limitado.

Criterio.- Cualquier software a instalarse deberá ser realizado por el área de monitoreo, el cual se asegurará que provenga de fuentes conocidas y seguras, además de cerciorarse de que dicha instalación no cree conflicto alguno.

Causa.- Los usuarios tienen perfil "Administrador" en el computador por lo cual pueden instalar cualquier tipo de software.

Efecto.- Afectar al rendimiento del computador del usuario así como también se pueden producir filtraciones de código malicioso de software no autorizado que pueden poner en riesgo la disponibilidad e integridad de la información, además del riesgo legal asociado al tener instalado software sin licencias autorizadas que puede crear demandas o problemas legales entre la institución y los propietarios de software.

Conclusión.- No se controla la aplicación de la política de seguridad referente a la instalación de software autorizado.

Recomendación.- El Director Ejecutivo deberá disponer que cambien el perfil de los usuarios con un perfil de privilegios limitados a fin de evitar la instalación de software no autorizado.

ELABORADO POR:	J.M	**FECHA:**	**10-06-2014**
REVISADO POR:	M.V	**FECHA:**	**12-06-2014**

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

HALLAZGOS N° 04

FUNCIONES Y RESPONSABILIDADES DEL PERSONAL

Condición.- No se encuentra determinada las funciones y responsabilidades de los encargados del departamento de control y monitoreo.

Criterio.- Tener definidas las funciones y responsabilidades del departamento de control y monitoreo.

Causa.- No se encuentran definidas las funciones y responsabilidades del personal de control y monitoreo. El cargo ha sido asignado a la jefa del Departamento de Control y Monitoreo en lo referente a la custodia de las claves de los servidores y base de datos principal, transportación de los respaldos a una ubicación externa, revisión de los logs y accesos otorgados a los usuarios e informe de estas revisiones al Director Ejecutivo.

Efecto.- Que los temas relacionados a la Seguridad de la Información no sean tratados con la debida diligencia, compromiso y de manera efectiva. La Administración de Usuarios está siendo manejada por el Departamento de Control y Monitoreo lo cual puede provocar conflictos de intereses y accesos no autorizados que pueden afectar a la confidencialidad e integridad de la información.

ELABORADO POR:	J.M	**FECHA:**	10-06-2014
REVISADO POR:	M.V	**FECHA:**	12-06-2014

Conclusión.- No se puede definir la responsabilidad del encargado de la Seguridad de la Información en los diferentes procesos en los que pueda intervenir.

Recomendación.- El Director Ejecutivo deberá definir que se apruebe formalmente el perfil del cargo del Oficial de Seguridad el cual debe pertenecer a un área independiente al Departamento de Control y Monitoreo reportar al Director Ejecutivo y en lo posible no ser usuario operativo de las aplicaciones a fin de evitar conflictos de intereses a través de la segregación de funciones.

ELABORADO POR:	J.M	**FECHA:**	**10-06-2014**
REVISADO POR:	M.V	**FECHA:**	**12-06-2014**

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

HALLAZGOS N° 05

CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN

Condición.- No existen políticas y procedimientos de clasificación y etiquetado de la información.

Criterio.- Política para la clasificación y etiquetado de la información.

Causa.- Al no existir políticas ni procedimientos para la clasificación y etiquetado en la información, puede a ver confusión en los mismos.

Efecto.- Accesos no autorizados a la información ya sea esta digital o física, lo cual puede provocar pérdida de la confidencialidad de la información.

Conclusión.- La información no se encuentra debidamente clasificada y etiquetada lo cual puede provocar pérdida de la confidencialidad de la información.

Recomendación.- El Director Ejecutivo deberá definir una política y procedimientos necesarios para una adecuada clasificación y etiquetado de la información así como de "escritorio limpio" (sin información confidencial a la vista) y capacitación a los empleados para el correcto uso de la información confidencial y de uso interno acorde a las necesidades de la entidad.

ELABORADO POR:	J.M	**FECHA:**	**10-06-2014**
REVISADO POR:	M.V	**FECHA:**	**12-06-2014**

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

HALLAZGOS N° 06

PROCESO DISCIPLINARIO

Condición.-No existe una política de seguridad para sancionar a los empleados.

Criterio.- Que exista un proceso disciplinario formal para los empleados que han comprometido una vulnerabilidad de seguridad.

Causa.- No existe un proceso disciplinario en casos de violaciones a las políticas de seguridad por parte de los empleados.

Efecto.- Incumplimiento a las políticas de seguridad sin poder sancionar a los responsables.

Conclusión.- Al no existir un proceso disciplinario, no se puede sancionar a los empleados que violen las políticas de seguridad comprometiendo la integridad, confidencialidad y disponibilidad de la información.

ELABORADO POR:	J.M	**FECHA:**	**10-06-2014**
REVISADO POR:	M.V	**FECHA:**	**12-06-2014**

Recomendación.- El Director Ejecutivo deberá incluir en la política de seguridad un proceso disciplinario para los empleados que violen la política de seguridad y que éstas sean difundidas a todo el personal a través de concienciación y capacitación continua así como revisiones independientes y periódicas para verificar el cumplimiento de la política y el respectivo reporte.

ELABORADO POR:	J.M	**FECHA:**	**10-06-2014**
REVISADO POR:	M.V	**FECHA:**	**12-06-2014**

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

HALLAZGOS N° 07

ACUERDOS DE CONFIDENCIALIDAD O NO REVELACIÓN

Condición.-No existen acuerdos de confidencialidad o no revelación en los contratos a los empleados.

Criterio.- Acuerdos de confidencialidad o no revelación junto a los términos y condiciones de los contratos.

Causa.- Al no establecer en los contratos acuerdos de confidencialidad o no revelación, existe fuga de información por parte de los empleados.

Efecto.- Fuga de información por parte de los empleados de la entidad ya que no les impide ningún argumento legal para no tomar información valiosa y aplicarla en otra entidad.

Conclusión.- No se puede garantizar la confidencialidad o no revelación de la información de los empleados hacia otras entidades.

Recomendación.- Al Director Ejecutivo que implemente una política para contratar el personal que va a laborar en la entidad, en la cual especifique en el contrato la confidencialidad y no revelación para evitar futuras fugas de información.

ELABORADO POR:	J.M	**FECHA:**	**10-06-2014**
REVISADO POR:	M.V	**FECHA:**	**12-06-2014**

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

HALLAZGOS N° 08

PLAN DE MANTENIMIENTOS DE EQUIPOS DE USUARIOS

Condición.-No existe un cronograma de actividades para el mantenimiento de equipos.

Criterio.- Plan de mantenimiento de equipos de usuarios.

Causa.- En el cronograma del Departamento de Control y Monitoreo no se evidencian actividades relacionadas al mantenimiento de equipos de los usuarios.

Efecto.- Daños inesperados en los computadores o servidores que pueden afectar a la disponibilidad e integridad de la información y a la continuidad de los procesos normales del negocio.

Conclusión.- No se puede garantizar el normal funcionamiento de los equipos al no realizarse los mantenimientos preventivos a los mismos.

Recomendación.- Al Director Ejecutivo que se establezca un plan de mantenimiento de los equipos de la institución que garanticen la disponibilidad de los equipos y la continuidad de las operaciones normales de la entidad.

ELABORADO POR:	J.M	**FECHA:**	**10-06-2014**
REVISADO POR:	M.V	**FECHA:**	**12-06-2014**

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO
AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

HALLAZGOS N° 09

PROTECCIÓN Y ASILAMIENTO DE LOS EQUIPOS

Condición.- No se encuentran los equipos protegidos al contacto de los usuarios.

Criterio.- Los equipos se aíslan o se protegen para reducir los riesgos de las amenazas y peligros medioambientales y para reducir las oportunidades de acceso no autorizado.

Causa.- Los servidores se encuentran ubicados en un gabinete cerrado dentro del Departamento de Sistemas la cual está separada por paredes falsas de madera, tela y aluminio y contigua a un área de archivos, sin embargo, si cuenta con extintor de incendio, detectores de humo, control de temperatura y humedad, sensores de movimiento, cerradura eléctrica, entre otros.

Efecto.- Fácil propagación del calor en caso de un siniestro al estar junto a un área en el que se guarda material de fácil combustión, lo cual puede comprometer la disponibilidad de los servicios de TI y la continuidad del negocio.

Conclusión.- El Departamento de Control y Monitoreo no se encuentra totalmente protegida y se encuentra junto a un área que almacena material de fácil combustión.

ELABORADO POR:	J.M	**FECHA:**	**10-06-2014**
REVISADO POR:	M.V	**FECHA:**	**12-06-2014**

Recomendación.- Al Director Ejecutivo que se aísle de mejor manera los servidores en un área de difícil acceso, si es posible fuera del Departamento de Control y Monitoreo que no esté expuesto a los riesgos medio ambientales a través de la implementación de un centro de cómputo que cumpla con todos los estándares de seguridad con normas que permitan su adecuada protección y alejado de áreas que almacenen materiales de fácil combustión.

ELABORADO POR:	J.M	**FECHA:**	**10-06-2014**
REVISADO POR:	M.V	**FECHA:**	**12-06-2014**

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

HALLAZGOS N° 10

ELIMINACIÓN Y REUTILIZACIÓN DE EQUIPOS

Condición.- No existen procedimientos para la eliminación de equipos o reutilización de los mismos.

Criterio.- Los equipos destinados a eliminación o reutilización, que contienen disco, suberifican previamente asegurando que toda la información delicada o el software licenciado se destruyen físicamente, o son sobrescritos de manera segura.

Causa.- No existe un procedimiento formal de eliminación de equipos y se pudo evidenciar que existen computadores que mantienen el nombre del computador identificado por el Departamento a la que pertenecieron anteriormente, lo que evidencia que no se ha aplicado un procedimiento para la reutilización de los mismos.

Efecto.- Accesos no autorizados a la información con la pérdida de confidencialidad que esto conlleva.

Conclusión.- No se puede garantizar que cuando los equipos son reutilizados o eliminados, exista información sensible que puede llegar a terceros no autorizados.

Recomendación.- Al Director Ejecutivo es establecer procedimientos para la eliminación o reutilización de los equipos y un departamento o función que permita la verificación de estos procedimientos a fin de garantizar la adecuada aplicación de los mismos (control de calidad).

ELABORADO POR:	J.M	**FECHA:**	**10-06-2014**
REVISADO POR:	M.V	**FECHA:**	**12-06-2014**

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

HALLAZGOS N° 11

RESPALDOS (BACK-UP)

Condición.- No se realizan respaldos de la base de datos.

Criterio.- Se deben realizar respaldos de la información y del software la de mayor impacto para la entidad.

Causa.- En el procedimiento de Respaldos diarios de la Base de Datos principal se indica que "el asistente del Departamento de Sistemas firma la bitácora de respaldos de base de datos para dejar constancia de que le han entregado el respaldo", sin embargo, no existe evidencia de la entrega del respaldo a la Jefa del Departamento de Sistemas. Los respaldos de los usuarios, así como las bases de datos de los aplicativos "satélites" (Monitoreos, Recursos Humanos, Contabilidad, que utilizan otras bases de datos y que se integran al Sistema principal a través de interfaces) no se almacenan en un lugar externo a la entidad.

Efecto.- Que no se pueda garantizar la continuidad de las operaciones en el caso de que suceda un siniestro y no se cuente con el último respaldo tanto de la base de datos como de las demás aplicaciones en una ubicación externa.

Conclusión.- No se está cumpliendo totalmente el procedimiento de Respaldos y no se está respaldando toda la información de los usuarios y aplicaciones "satélites" en un lugar externo.

ELABORADO POR:	J.M	**FECHA:**	**10-06-2014**
REVISADO POR:	M.V	**FECHA:**	**12-06-2014**

Recomendación.- El Director Ejecutivo deberá analizar la factibilidad de que los respaldos sean enviados al casillero de seguridad a través de un tercero al ser información de la entidad sensible y confidencial de tal forma que se garantice la responsabilidad de llevar los mismos a la ubicación externa; el Departamento de Control y Monitoreo es la responsable del control interno verificando que el procedimiento de respaldo se cumpla con la periodicidad e información definida y no debería tener la responsabilidad del traslado de los respaldos pues entraría en conflicto de intereses por una inadecuada segregación de funciones, la información respaldada debe ser la de mayor relevancia ya que su costo es elevado.

Los respaldos de los usuarios y de las bases de datos de los aplicativos "satélites" también deben almacenarse en una ubicación externa en la periodicidad que determine el Director Ejecutivo de acuerdo a las necesidades de la entidad.

ELABORADO POR:	J.M	**FECHA:**	**10-06-2014**
REVISADO POR:	M.V	**FECHA:**	**12-06-2014**

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

HALLAZGOS N° 12

ACEPTACIÓN DEL SISTEMA

Condición.- No existen criterios de aceptación para los sistemas de información, actualizaciones y versiones nuevas.

Criterio.- Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas de los sistemas durante su desarrollo y antes de su aceptación.

Causa.- No se pudo evidenciar la existencia de un plan de pruebas para los cambios que se realizan en los sistemas; existe el "Formulario de Control de Versiones de Software" en el cual solo se menciona que se han realizado las pruebas con el usuario y su aceptación, pero no se indican qué pruebas fueron realizadas.

Efecto.- Modificaciones no autorizadas o mal intencionadas que pueden afectar a la integridad o disponibilidad de la información que se encuentra en las bases de datos.

Conclusión.- El procedimiento de "Desarrollo de Software", en la fase de "Pruebas" no indica qué tipo de pruebas y la forma de documentar las mismas.

ELABORADO POR:	J.M	**FECHA:**	**10-06-2014**
REVISADO POR:	M.V	**FECHA:**	**12-06-2014**

Recomendación.- Al Director Ejecutivo deberá modificar el procedimiento de "Desarrollo de Software" en la fase de "Pruebas" indicando: Procedimiento del Plan de pruebas, formulario requerido para dejar evidencia de la realización de las mismas, lista de verificación con las pruebas mínimas que deben ser realizadas y que estas pruebas las realice una persona diferente a la que desarrolló el cambio.

ELABORADO POR:	J.M	**FECHA:**	**10-06-2014**
REVISADO POR:	M.V	**FECHA:**	**12-06-2014**

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

HALLAZGOS N° 13

CONTROL DE ACCESOS

Condición.- No existe un procedimiento formal de entrega/ recepción de claves para los usuarios.

Criterio.- La asignación de claves se debe controlar a través de un proceso de gestión formal.

Causa.- Falta de gestión para aplicar un procedimiento formal de entrega/recepción de las claves de usuario.

Efecto.- Se pueden crear accesos no autorizados que afecten a la integridad y confidencialidad de la información.

Conclusión.- El procedimiento no garantiza una correcta gestión en la entrega de claves.

Recomendación.- Al Director Ejecutivo debe crear el procedimiento formal para entrega de contraseñas, dejando un registro de la entrega/recepción de la clave y la responsabilidad sobre la misma.

ELABORADO POR: J.M	**FECHA:** 10-06-2014
REVISADO POR: M.V	**FECHA:** 12-06-2014

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

HALLAZGOS N° 14

REPORTE DE LA SEGURIDAD DE LA INFORMACIÓN

Condición.- No existe un procedimiento formal que asegure el reporte al Director Ejecutivo.

Criterio.- Asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.

Causa.- No existe un procedimiento formal que asegure el reporte al Director Ejecutivo de los incidentes que puedan poner en riesgo la Seguridad de la Información.

Efecto.- Que se produzcan incidentes de seguridad que pueden afectar a la integridad, confidencialidad y disponibilidad de la información.

Conclusión.- Al no existir un procedimiento para reportar los incidentes de seguridad, no se pueden tomar las medidas correctivas necesarias.

Recomendación.- El Director Ejecutivo deberá crear políticas y procedimientos formales para la gestión de incidentes, así como la asignación de la responsabilidad de reportarlos al Director Ejecutivo a fin de tomar medidas correctivas o de mejora. Estos reportes de incidentes deben incluir al menos: forma en que inició el incidente, vulnerabilidades explotadas, forma de detección, solución temporal, responsable de la detección del incidente entre otros.

ELABORADO POR: J.M	**FECHA:** 10-06-2014
REVISADO POR: M.V	**FECHA:** 12-06-2014

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

HALLAZGOS N° 15

PROCESOS CLAVES PARA LA CONTINUIDAD DEL NEGOCIO

Condición.- No existen procedimientos manuales de los procesos claves para la continuidad del negocio.

Criterio.- Se debe mantener un solo marco referencial de planes de continuidad para asegurar que todos los planes sean consistentes y para tratar consistentemente los requerimientos de la seguridad de la información e identificar las pruebas y mantenimiento.

Causa.- No existe una metodología o marco referencial formalmente establecido y aprobado que garantice el proceso de Administración de la Continuidad del Negocio. No existe evidencia de la capacitación realizada en los temas relacionados, tampoco se detallan las actividades a realizar por cada uno de los responsables pues están descritas de manera general. No están definidos los procedimientos y formularios manuales que se van a utilizar cuando ocurra un evento que ponga en riesgo la continuidad de las operaciones, ni las políticas y procedimientos que van a regir durante la contingencia.

Efecto.- Que no se puedan integrar los planes de contingencia departamentales en el momento de una interrupción del negocio. Que la aplicación del plan no sea efectiva afectando la continuidad del negocio.

ELABORADO POR:	J.M	**FECHA:**	**10-06-2014**
REVISADO POR:	M.V	**FECHA:**	**12-06-2014**

Conclusión.- No existe un plan de continuidad de negocio estructurado que contiene: Análisis de Impacto del negocio, procedimientos de recuperación de las Bases de Datos y aplicaciones críticas, política de mantenimiento y el resultado de la última prueba realizada. Sin embargo, no todo el personal ha sido capacitado en los procedimientos a realizarse en caso de una contingencia mayor que comprométala continuidad del negocio, tampoco han sido definidas las políticas y procedimientos que van a regir durante la contingencia, lo cual podría afectar a la ejecución del plan.

Recomendación.- El Director Ejecutivo deberá crear la metodología de la Planeación de la continuidad a fin de alinear los planes departamentales con el plan de continuidad del negocio general que tiene la institución y se pueda crear el proceso de Administración de la Continuidad del negocio. Esta metodología debe incluir al menos los siguientes temas:

- Análisis de Impacto del Negocio (que si se lo ha hecho actualmente).
- Definición de Estrategias de recuperación.
- Forma de implantar la estrategia de recuperación y responsables de la misma.
- Plan de Pruebas y mantenimiento del Plan de Continuidad del Negocio.

ELABORADO POR: J.M	**FECHA:** 10-06-2014
REVISADO POR: M.V	**FECHA:** 12-06-2014

El Director Ejecutivo debe estar consciente que la Continuidad del negocio es un proceso que pertenece no solamente al Departamento de Control y Monitoreo sino a toda la institución, el mismo que debe ser retroalimentado a partir de las pruebas realizadas para analizar las brechas a fin de que su aplicación sea efectiva y eficiente.

Se sugiere al Director Ejecutivo que el Plan de continuidad del negocio sea actualizado, aprobado y difundido al personal cada vez que se realicen cambios en los colaboradores responsables de la ejecución del mismo o se implementen nuevos procesos críticos; además se debe detallar las actividades y procedimientos a seguir por cada uno de los responsables durante la ejecución del plan. Cabe mencionar que este Plan de continuidad debe respaldarse en un lugar externo a la entidad para garantizar su disponibilidad y fácil acceso en caso de una contingencia o siniestro.

ELABORADO POR:	J.M	**FECHA:**	**10-06-2014**
REVISADO POR:	M.V	**FECHA:**	**12-06-2014**

MORALES & VALLE ASOCIADOS
AUDITORES INDEPENSIENTES CIA. LTDA

LC

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

JUNIO 2014

FASE IV – COMUNICACIÓN DE RESUTADOS

INFORME FINAL DE AUDITORÍA

INDICE

ELABORADO POR:	J.M	**FECHA:**	24-06-2014
REVISADO POR:	M.V	**FECHA:**	25-06-2014

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

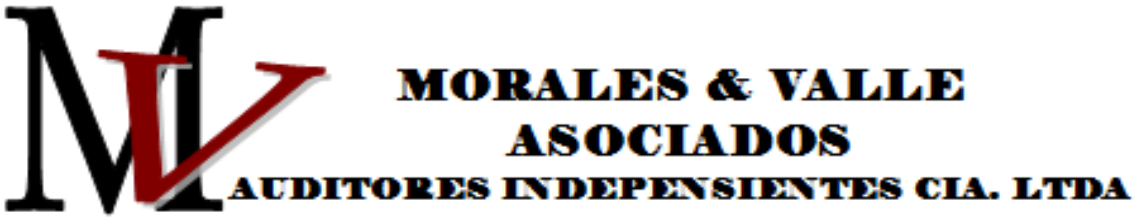
AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

PROGRAMA DE AUDITORÍA – INFORME FINAL DE AUDITORÍA

N°	DESCRIPCIÓN	REF P/T	REALIZADO POR:	FECHA
	OBJETIVOS:			
1	Determina las respectivas conclusiones y recomendaciones para exponer Director Ejecutivo de la Entidad el Ing. Edwin Niamiña el informe de auditoría.			
	PROCEDIMIENTOS:			
1	Informe final de Auditoría Informática de la Seguridad de la Información.	$HH^{1}/_{24}$-$^{24}/_{24}$	IA	07-06-2014

ELABORADO POR:	J.M	**FECHA:**	24-06-2014
REVISADO POR:	M.V	**FECHA:**	25-06-2014

4.7.3 Informe Final de Auditoria



RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

INFORME FINAL AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

PERIODO

ENERO 2012 – DICIEMBRE 2012

MORALES & VALLE
ASOCIADOS
AUDITORES INDEPENSIENTES CIA. LTDA

Riobamba, 19 de Junio del 2014

Señor

Ing. Edwin Niamiña Lara
DIRECTOR EJECUTIVO DE LA RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO.
Presente

De mi consideración

Hemos efectuado la Auditoría de la Seguridad de la Información al Departamento de Control y Monitoreo de la Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo (REFICH) de la ciudad de Riobamba, provincia de Chimborazo, periodo 2012.

El examen se efectuó de acuerdo a las Normas ISO 17799 en relación a la Seguridad de la Información emitidas por la Organización Internacional de Estandarización, dicho examen requiere que sea planificado y ejecutado, a fin de obtener la certeza razonable de que la información y documentación revisada no contiene exposiciones erróneas de carácter significativo, de conformidad con las disposiciones legales y reglamentarias vigentes, políticas y demás normas aplicables.

Debido a la naturaleza del examen, los resultados se encuentran expresados en las conclusiones y recomendaciones que consta en el presente informe.

Atentamente

Srta. Ma. Lorena Valle Romero
Supervisor

INFORMACIÓN INTRODUCTORIA

MOTIVOS DE LA AUDITORÍA

La Auditoría de la Seguridad de la Información a la Red de Estructura de Finanzas Populares y Solidarias de Chimborazo de la ciudad de Riobamba, provincia de Chimborazo, periodo 2012, se llevó a cabo con la finalidad de medir el grado de cumplimiento de normativas vigentes en relación a la Seguridad de la Información.

OBJETIVOS DE LA AUDITORÍA

- Realizar un análisis bibliográfico documental respecto a la Auditoría Informática, sistema de información y la norma ISO/IEC 17799 como elementos que direccionen la investigación.

- Evaluar el sistema de información en la Red de Estructura de Finanzas Populares y Solidarias de Chimborazo aplicando la norma ISO/IEC 17799.

- Emitir informe de auditoría con recomendaciones para el mejoramiento del Departamento de Control y Monitoreo.

ENFOQUE DE LA AUDITORÍA

El examen de Auditoría está orientado hacia el cumplimiento de las normativas en relación a la Seguridad de la Información del Departamento de Control y Monitoreo de la Entidad.

ACIÓN DE LA ENTIDAD

ANTECEDENTES

La Personería Jurídica a REFICH fue emitida por el Ministerio de Industrias y Productividad (MIPRO), en la ciudad de Ambato, Acuerdo Ministerial No. 09432 con fecha del 25 de noviembre de 2009, después de haber cumplido con todos los requisitos legales para la adjudicación de la Personería Jurídica.

REFICH se constituye como una organización de segundo piso que apoya, coordina y ejecuta procesos alternativos de intermediación financiera con Estructuras Financieras Populares y Locales en la provincia de Chimborazo, que fomenta la unión, responsabilidad, confianza y la solidaridad de sus 18 Filiales ubicada en los cantones: Alauís, Pallatanga, Colta, Guamote, Riobamba, Chambo, Guano y Chunchi.

La ciudad de Riobamba el 11 y 12 de diciembre del año 2009, se constituyó en el escenario de encuentro y discusión de los diferentes representantes de Cajas, Bancos y Grupos Solidarios del país, en donde discutieron y analizaron la propuesta del Proyecto de Ley del Sistema Financiero Popular y Solidario, ante la desigual participación de este tipo de organizaciones locales dentro de las estructuras legales; para crear los espacios y la oportunidad de que este sector exponga sus experiencias, necesidades y presenten alternativas válidas para la construcción de un frente activo que permita incorporar sus realidades a la discusión de dicho proyecto de Ley.

Considerada por sus Filiales como un espacio democrático de integración y cooperación mutua entre cooperativas, cajas de ahorro y crédito y grupos asociativos, creada para fortalecer el trabajo de las Estructuras Financieras Locales filiales que son actores indiscutibles de la Economía Popular y Solidaria, a través de la capacitación, asistencia técnica y asesoramiento, comprometidos con el Desarrollo Económico Local de las comunidades, parroquias y cantones a los que pertenecen.

MISION:

La Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo es una organización integradora conformada por Estructuras Financieras Locales que tienen objetivos comunes y basa su trabajo en principios y valores, articulando servicios financieros y no financieros entre sus filiales, impulsando el desarrollo socio-económico de la provincia con representatividad local e incidencia nacional.

VISION:

Al 2013 la Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo es una organización ética, social y financieramente sostenible que promueve el desarrollo socio económico de los territorios rurales y urbano marginales de la provincia brindando servicios financieros y no financieros de calidad que responden a las necesidades y oportunidad de sus filiales.

RESULTADOS ESPECÍFICOS POR COMPONENTES

1. **SE HA DETERMINADO QUE NO EXISTEN POLÍTICAS DE SEGURIDAD ACTUALIZADAS.**

Las políticas de seguridad no se encuentran actualizadas.

Recomendación.- El Director Ejecutivo deberá disponer que el Departamento de Control y Monitoreo realice revisiones periódicas a la política de seguridad cada vez que se realicen cambios significativos en la tecnología o en los procedimientos del área de Sistemas así como revisiones que permitan verificar el cumplimiento de la Política de Seguridad debe ser una directriz general para una adecuada administración de la Seguridad de la Información de la entidad.

2. **SE HA EVIDENCIADO LA NO EJECUCIÓN AUTOMÁTICA DEL ANTIVIRUS.**

Existen computadores infectados en la entidad.

Recomendación.- El Director Ejecutivo deberá disponer al Departamento de Control monitoreo que incluya en su programa anual la revisión periódica del cumplimiento de la política de seguridad verificando la correcta implementación de los controles necesarios para su aplicabilidad.

3. **SE HA COMPROBADO LA FALTA DE CONTROL EN LOS USUARIOS DE PERFIL.**

Los usuarios poseen un perfil de administrador, por lo tanto su perfil no es limitado.

Recomendación.- El Director Ejecutivo deberá disponer que cambien el perfil de los usuarios con un perfil de privilegios limitados a fin de evitar la instalación de software no autorizado.

4. LA ENTIDAD NO CUENTA CON FUNCIONES Y RESPONSABILIDADES DEFINIDAS DEL PERSONAL

No se encuentra determinada las funciones y responsabilidades del encargado de la seguridad de información.

Recomendación.- El Director Ejecutivo deberá definir que se apruebe formalmente el perfil del cargo del Oficial de Seguridad el cual debe pertenecer a un área independiente al Departamento de Control y Monitoreo reportar al Director Ejecutivo y en lo posible no ser usuario operativo de las aplicaciones a fin de evitar conflictos de intereses a través de la segregación de funciones.

5. FALTA DE CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN

No existen políticas y procedimientos de clasificación y etiquetado de la información.

Recomendación.- El Director Ejecutivo deberá definir una política y procedimientos necesarios para una adecuada clasificación y etiquetado de la información así como de "escritorio limpio" (sin información confidencial a la vista) y capacitación a los empleados

para el correcto uso de la información confidencial y de uso interno acorde a las necesidades de la entidad.

6. LA ENTIDAD NO APLICA UN PROCESO DISCIPLINARIO

No existe una política de seguridad para sancionar a los empleados.

Recomendación.- El Director Ejecutivo deberá incluir en la política de seguridad un proceso disciplinario para los empleados que violen la política de seguridad y que éstas

sea n dif und idas a todo el personal a través de concienciación y capacitación continua así como revisiones independientes y periódicas para verificar el cumplimiento de la política y el respectivo reporte.

7. INEXISTENCIA DE ACUERDOS DE CONFIDENCIALIDAD O NO REVELACIÓN

No existen acuerdos de confidencialidad o no revelación en los contratos a los empleados.

Recomendación.- Al Director Ejecutivo que implemente una política para contratar el personal que va a laborar en la entidad, en la cual especifique en el contrato la confidencialidad y no revelación para evitar futuras fugas de información.

8. SE HA DETERMINADO QUE NO SE CUENTA CON UN PLAN DE MANTENIMIENTOS DE EQUIPOS DE USUARIOS.

No existe un cronograma de actividades para el mantenimiento de equipos.

Recomendación.- Al Director Ejecutivo que se establezca un plan de mantenimiento de los equipos de la institución que garanticen la disponibilidad de los equipos y la continuidad de las operaciones normales de la entidad.

MORALES & VALLE ASOCIADOS
AUDITORES INDEPENSIENTES CIA. LTDA

9. EXISTE INSEGURIDAD EN LA PROTECCIÓN Y ASILAMIENTO DE LOS EQUIPOS.

No se encuentran los equipos protegidos al contacto de los usuarios.

Recomendación.-Al Director Ejecutivo que se aísle de mejor manera los servidores en un área de difícil acceso, si es posible fuera del Departamento de Control y Monitoreo que no esté expuesto a los riesgos medio ambientales a través de la implementación de un centro de cómputo que cumpla con todos los estándares de seguridad con normas que permitan su adecuada protección y alejado de áreas que almacenen materiales de fácil combustión.

10. LA ENTIDAD NO HA ESTABLECIDO PROCEDIMIENTOS PARA ELIMINACIÓN Y REUTILIZACIÓN DE EQUIPOS

No existen procedimientos para la eliminación de equipos o reutilización de los mismos.

Recomendación.- Al Director Ejecutivo es establecer procedimientos para la eliminación o reutilización de los equipos y un departamento o función que permita la verificación de estos procedimientos a fin de garantizar la adecuada aplicación de los mismos (control de calidad).

11. EL PERSONAL NO REALIZA RESPALDOS (BACK-UP).

No se realizan respaldos de la base de datos.

Recomendación.- El Director Ejecutivo deberá analizar la factibilidad de que los respaldos sean enviados al casillero de seguridad a través de un tercero al ser información de la entidad sensible y confidencial de tal forma que se garantice la responsabilidad de llevar

los mismos a la ubicación externa; el Departamento de Control y Monitoreo es la responsable del control interno verificando que el procedimiento de respaldo se cumpla con la periodicidad e información definida y no debería tener la responsabilidad del traslado de los respaldos pues entraría en conflicto de intereses por una inadecuada segregación de

funciones, la información respaldada debe ser la de mayor relevancia ya que su costo es elevado.

Los respaldos de los usuarios y de las bases de datos de los aplicativos "satélites" también deben almacenarse en una ubicación externa en la periodicidad que determine el Director Ejecutivo de acuerdo a las necesidades de la entidad.

12. FALTA DE CRITERIOS DE ACEPTACIÓN DEL SISTEMA.

No existen criterios de aceptación para los sistemas de información, actualizaciones y versiones nuevas.

Recomendación.- Al Director Ejecutivo deberá modificar el procedimiento de "Desarrollo de Software" en la fase de "Pruebas" indicando: Procedimiento del Plan de pruebas, formulario requerido para dejar evidencia de la realización de las mismas, lista de verificación con las pruebas mínimas que deben ser realizadas y que estas pruebas las realice una persona diferente a la que desarrolló el cambio.

13. ENTREGA INADECUADA DE CLAVES AL PERSONAL

No existe un procedimiento formal de entrega/ recepción de claves para el personal.

Recomendación.- Al Director Ejecutivo debe crear el procedimiento formal para entrega de contraseñas, dejando un registro de la entrega/recepción de la clave y la responsabilidad sobre la misma.

14. SE HA VERIFICADO LA NO REALIZACIÓN DE UN REPORTE EN LA SEGURIDAD DE LA INFORMACIÓN

No existe un procedimiento formal que asegure el reporte al Director Ejecutivo.

Recomendación.- El Director Ejecutivo deberá crear políticas y procedimientos formales para la gestión de incidentes, así como la asignación de la responsabilidad de reportarlos al Director Ejecutivo a fin de tomar medidas correctivas o de mejora. Estos reportes de incidentes deben incluir al menos: forma en que inició el incidente, vulnerabilidades explotadas, forma de detección, solución temporal, responsable de la detección del incidente entre otros.

15. SE COMPROBO LA FALATA DE PROCESOS CLAVES PARA LA CONTINUIDAD DEL NEGOCIO

No existen procedimientos manuales de los procesos claves para la continuidad del negocio.

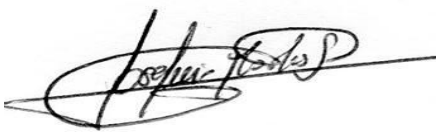
Recomendación.- El Director Ejecutivo deberá crear la metodología de la Planeación de la continuidad a fin de alinear los planes departamentales con el plan de continuidad del negocio general que tiene la institución y se pueda crear el proceso de Administración de la Continuidad del negocio. Esta metodología debe incluir al menos los siguientes temas:

- Análisis de Impacto del Negocio (que si se lo ha hecho actualmente).
- Definición de Estrategias de recuperación.
- Forma de implantar la estrategia de recuperación y responsables de la misma.
- Plan de Pruebas y mantenimiento del Plan de Continuidad del Negocio.

El Director Ejecutivo debe estar consciente que la Continuidad del negocio es un proceso que pertenece no solamente al Departamento de Control y Monitoreo sino a toda la

institución, el mismo que debe ser retroalimentado a partir de las pruebas realizadas para analizar las brechas a fin de que su aplicación sea efectiva y eficiente.

Se sugiere al Director Ejecutivo que el Plan de continuidad del negocio sea actualizado, aprobado y difundido al personal cada vez que se realicen cambios en los colaboradores responsables de la ejecución del mismo o se implementen nuevos procesos críticos; además se debe detallar las actividades y procedimientos a seguir por cada uno de los responsables durante la ejecución del plan. Cabe mencionar que este Plan de continuidad debe respaldarse en un lugar externo a la entidad para garantizar su disponibilidad y fácil acceso en caso de una contingencia o siniestro.



Srta. Ma. Lorena Valle Romero — Sr. Jose L. Morales Garcés

SUPERVISOR — **AUDITOR**

CONCLUSIONES

✓ Una vez efectuada la Auditoría Informática en la Seguridad de la Información en el Departamento de Control y Monitoreo de la Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo, podemos determinar que se han cumplido con los objetivos planteados en esta tesis, los que a continuación detallamos:

1.- Se realizó el análisis bibliográfico documental respecto a la Auditoría Informática, Sistema de Información y la norma ISO/IEC 17799.
2.- Se evaluó el Sistema de Información en la Red de Estructura de Finanzas Populares y Solidarias de Chimborazo aplicando la norma ISO/IEC 17799.
3.- Se emitió el informe de auditoría con recomendaciones para el mejoramiento en el Departamento de Control y Monitoreo.

- ✓ Hemos establecido un modelo de evaluación para próximas auditorías donde se facilita la identificación de puntos vulnerables y errores en el Departamento de Control y Monitoreo de la Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo.

- ✓ Con la realización de la tesis, la Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo podrá tomar las medidas correctivas pertinentes a cada uno de los casos encontrados cumpliendo con el propósito de proteger la información.

- ✓ Con el análisis de la utilización de la norma ISO/IEC 17799 en otras entidades determinamos que la REFICH, debería aplicar para una mejor supervisión y lograr un alto rendimiento y mejora de la Seguridad de la Información.

RECOMENDACIONES

Al Director Ejecutivo de la Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo

- ✓ Aplicar las normas de la Seguridad de la Información ISO/IEC 17799 emitida por la Organización Internacional de Estandarización, las cuales adoptan las entidades, con la

finalidad de mantener el ordenado proceso de la Seguridad de la Información, en la Red de Estructuras de Finanzas Populares y Solidarias de Chimborazo.

✓ Aprovechar las sugerencias realizadas en el informe de Auditoría Informática de la Seguridad de la Información bajo las normas ISO/IEC 17799 que se detalla a continuación:

1.- Implementar el equipo tecnológico suficiente para poder cumplir las tareas diarias del trabajo, planificar capacitaciones constantes al personal encargado del Departamento de Control y Monitoreo durante el año, para brindar un mejor rendimiento al usuario de la Red de Estructura Financiera y Solidaria de Chimborazo.

2.- Adecuar la infraestructura y mobiliario para lograr un adecuado desenvolvimiento del personal en las actividades laborales, coordinar con el personal en una agenda institucional para la realización de un manual de control interno para las operaciones del Departamento de Control y Monitoreo de la Red de Estructura Financiera y Solidaria de Chimborazo.

BIBLIOGRAFÍA

Ávila, F. (1997). *Auditoría de Sistemas en empresas estatales.* México: Universidad de Valle de México.

Castro, T. J. (2010). *Compilación Bibliográfica ISO serie 27000, ISO 17799.* Manizales: Universidad de Caldas.

Cervantes, B. J. (2011). *Auditoría de la Seguridad de la Información de una Sociedad Financiera.* Guayaquil: Diplomado, ESPOL.

Echenique, J. (1988). *Auditoría en Sistemas* (2a ed.). México: McGraw/Hill.

FISMA. (2002). *Ley Federal de Gestión de Seguridad de la Información.* Washington.: 107o Congreso de los Estados Unidos.

Fuenzalida, D. l. (2005). *Aplicación de la Norma ISO/IEC 17799.* Santiago de Chile: Tesis, Universidad de Santiago de Chile.

Hernández, E. (2002). *Auditoría Informática Un enfoque metodológico y prática.* México: Continental.

Holmes, A. (1984). *Auditoría Principios y Procedimientos* (5a ed.). México: McGraw/Hill.

León, M. (2013). *Proceso de la Auditoría Financiera*. Loja: Ediloja.

Mair, W. (1987). *Auditoría Informática.* Washington:s.e.

Mariño, O. A. (2010). *Factores Inhibidores en la Implementación de Sistema de Gestión de la Seguridad de la Información.* Lima: s.e.

Muñoz, R. C. (2002). *Auditoría en Sistemas Computacionales*. México: Pearson Education.

OBM. (2008). *Oficina de Administración y Presupuesto.* Washington: Circular A-130.

Partida, & Ezingeard. (2007). *Critical Success Factors and Requirements for Achieving Business Benefits from in Formation Security.* Reino Unido: Henley Management.

Piattini, M., & Del Peso, E. (1998). *Auditoría Informática Un Enfoque Prático* (2a ed.). México:Alfaomega.

Porter, W., & Burton, J. (1983). *Auditoría en un Enfoque Conceptual.* México: Limusa.

Poveda, J. M. (2012). *Auditoría en Sistemas* . México: UNI-RUACS.

Sánchez, C. G. (2006). *Auditoría de Estados Financieros Práctica Moderna Integral* (2a ed.). México: Ibazeta.

Torres, B. M. (2007). *Plan de Implementación de un Sistema de Seguridad de la información.* Quito: Tesis.

Vargas, A. J. (2009). *Conceptos Básico de Auditoría Informática.* México: Universidad Nacional de Ingeniería.

Vethius. (2008). *Seguridad de la Información.*Washington*:* s.e.

Villalón, H. A. (2004). *Código de buenas prácticas de Seguridad ISO/IEC 17799*. Madrid: Grupo S2.

Weber, R. (1982). *Auditing Conceptual Foundations and Practice.* Washington.: s.e.

Yann. (1998). *Técnicas de Auditoría.*Washington: s.e.

LINKOGRAFÍA

AAS. Recuperado (30 de marzo de 2014). *American Accounting Association*. Obtenido de AAA: www.aaahq.org

Aenor. Recuperado (30 de marzo de 2014). *Asociación Española de Normalización y Certificación*. Obtenido de Aenor: www.aenor.es

AICPA. Recuperado (30 de marzo de 2014). *Instituto Norteamericano de Contadores Públicos*. Obtenido de AICPA: www.aicpa.org

ASIMELEC. Recuperado (28 de marzo de 2014). *Asociación Multisectorial de Empresas de Tecnologías de la Información, Comunicaciones y Electrónica*. Obtenido de Asimelec: www.asimelec.es

BSI. Recuperado (30 de marzo de 2014). Bristish Standards Institution. *Management System 2001 ¿Que es la norma ISO/IEC 17799?* Reino Unido: BSI.

Ernst, & Young's. Recuperado (30 de marzo de 2014). *Ernst*. Obtenido de www.ey.ecom

Humphrey, T. Recuperado (7 de julio de 2014). *Financial Tech Magazine*. Obtenido de www.iso.org

ISO. Recuperado (30 de marzo de 2014). *International Organization for Standardization*. Obtenido de ISO: www.iso.org

PCM. Recuperado (30 de marzo de 2014). *Presidencia del Consejo de Ministros*. Obtenido de www.pcm.gob.pe

Survey. Recuperado (30 de marzo de 2014). *The Iso Survey*. Obtenido de www.theisosurvey.com

Survey, T. I. Recuperado (30 de marzo de 2014). *ISO Survey*. Obtenido de www.iso.org/iso/survey

UNIVA. Recuperado (30 de marzo de 2014). *Universidad del Valle de Atemajac*. Obtenido de www.univa.mx

GLOSARIO

Auditoría Interna.- Cuando es ejecutada por auditores de las unidades de auditoría interna de las entidades y organismos del sector público y de las entidades privadas. Las entidades y organismos del Sector Público como del sector privado de acuerdo a sus necesidades, complejidad de funciones y de conformidad a las disposiciones legales vigentes, contarán con una unidad de Auditoría Interna.

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

Sistema Informático.- Es el conjunto de elementos o componentes interconectados o relacionados para el tratamiento de información.

Información.- Es la comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre alguna materia determinada, podría entenderse que si no se consigue alguna de las dos finalidades señaladas, no habría tal información, pero es prácticamente imposible que no concurra alguna de ellas cuando un ser humano se encuentra ante una exposición de conocimientos.

Alcance de la auditoría.- El marco o límite de la auditoría y las materias, temas, segmentos o actividades que son objeto de la misma.

Control interno.- Son todas las medidas que una empresa utiliza para protegerse contra errores, desperdicios o fraudes, con el fin de mantener la confiabilidad de los datos contables, lo cual está diseñado para ayudar a la operación eficiente de una empresa y para asegurar el cumplimiento de las políticas de la empresa.

Salvaguardar los bienes.- Consideraremos como "bienes" de un Centro de Proceso de Datos (CPD) el hardware, software, personas, datos (ficheros, bases de datos, etc.), documentación, suministros, etc. Además, estos bienes se concentran todos en un mismo

sitio, el ámbito físico del CPD, por lo que deben de ser especialmente protegidos por un sistema de control interno, y su protección debe de ser un objetivo prioritario para la organización.

Integridad de datos.- Ya hemos visto que uno de los aspectos que debemos cuidar especialmente es la integridad de los datos, pero realizar esta tarea nos va a suponer un coste frente a los beneficios esperados al implantar unas medias de seguridad, desde de un punto de vista puramente empresarial, estos beneficios deben de superar los costes de implantación, para que sea rentable su utilización. Las veces en que el dato es usado por personas que toman decisiones. Si el dato es compartido, su falta de integridad afectará a todos los usuarios, por lo que en un entorno compartido es vital mantener esta integridad.

Toma de decisiones incorrecta.- Los datos nos van a permitir entre otras cosas realizar tomas de decisiones. Pero para que las decisiones tomadas a partir de los datos sean correctas, tendremos que garantizar que los datos que nos son suministrados son asimismo correctos.

Privacidad de los Datos.- Desde siempre se han recogido datos de personas para su uso comercial: datos personales, médicos, de impuestos, etc. Pero desde la llegada de los ordenadores la difusión "incontrolada" de estos datos se ha convertido en un serio problema, principalmente debido a que crear, actualizar y difundir una base de datos con datos personales de posibles clientes es mucho más fácil ahora que cuando los sistemas eran manuales.

Eficacia.- El grado en que se cumplen los objetivos y la relación entre el efecto deseado en una actividad y su efecto real.

Eficiencia.- La relación que existe entre el producto (en término de bienes, servicios u otros resultados) y los recursos empleados en su producción

Hallazgos.- Son el resultado de un proceso de recopilación y síntesis de información, la suma y la organización lógica de información relacionada con la entidad, actividad,

situación o asunto que se haya revisado o evaluado para llegar a conclusiones al respecto o para cumplir alguno de los objetivos de la auditoría.

Normas de auditoría.- Constituyen el conjunto de reglas que deben cumplirse para realizar una auditoría con la calidad y eficiencias indispensables.

Informe de auditoría.- Expresión escrita por el auditor respecto a los resultados de las verificaciones realizadas durante la ejecución de la auditoría, manifestando sus criterios y comentarios respecto a los estados financieros y otros hechos económicos.

Procedimiento de auditoría.- Las acciones que realiza el auditor para llevar a cabo sus labores de revisión.

Técnicas de auditoría.- Métodos que el auditor emplea para realizar las verificaciones planteadas en los programas de auditoría, que tienen como objetivo la obtención de evidencia.

ANEXOS

Anexo 1

MORALES & VALLE
ASOCIADOS
AUDITORES INDEPENSIENTES CIA. LTDA

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

AUTORIDAD DE LA ENTIDAD

ENTREVISTA – Ing. Edwin Niamiña

OBJETIVO: Conocer las instalaciones, actividades y situación actuales de la Entidad, así como del conocimiento que tiene como autoridad REFICH.

1. **RAZÓN SOCIAL**:

2. **FECHA DE CRACION DE LA INSTITUCIÓN:**

3. **DIRECCIÓN:**

4. **PROVINCIA:**

5. **CANTÓN:**

6. **PARROQUIA:**

7. **HORARIO DE ATENCIÓN:**

8. **- TELÉFONOS:**

9. **AUTORIDADES:**

Presidenta:

Director Ejecutivo:

10. FUNCIONES Y ATRUBUCIONES:

11. NÚMERO DE PERSONAS EN LA ENTIDAD:

12. CUENTA CON ESPACIO PROPIO EL DEPARTAMENTO DE CONTROL Y MONITOREO:

PREGUNTAS CERRADAS

7. ¿El presupuesto asignado a la Entidad por parte de la Asamblea de Socios es adecuado?

SI:

NO:

8. ¿El porcentaje que la Entidad destina al departamento cubre con las necesidades?

SI:

NO:

9. ¿El número de encargados del departamento es adecuado?

SI:

NO:

10. ¿Existe alguna persona responsable del departamento de control y monitoreo?

SI:

NO:

11. ¿Anteriormente se han realizado Auditorías Informáticas a la seguridad de la información de la Entidad?

SI:

NO:

12. *¿Cuenta la Entidad con un manual de funciones*?

SI:

NO:

GRACIAS POR LA ATENCIÓN

Anexos 2

MORALES & VALLE
ASOCIADOS
AUDITORES INDEPENSIENTES CIA. LTDA

RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

DEPARTAMENTO DE CONTROL Y MONITOREO

ENTREVISTA – Ing. Lorena Moreno

OBJETIVO: Conocer las instalaciones, actividades y situación en el área informática de la Institución.

1. ¿Cuántos computadores tiene el departamento de Control y Monitoreo de la REFICH?

2. ¿Cuál es el número de encargados del departamento?

3. ¿El lugar donde se encuentra ubicado el departamento está seguro de inundaciones, robos o cualquier otra situación que ponga en peligro los equipos informáticos?

PREGUNTAS CERRADAS

11. ¿Cree usted que la infraestructura física es adecuada?

SI ☐ ***NO*** ☐

12. ¿El mobiliario abastece para el trabajo realizado en el departamento?

SI ☐ ***NO*** ☐

13. ¿Se aplica normas de control interno al manejo de la información del departamento?

SI ☐ ***NO*** ☐

14. ¿Se realiza mantenimiento preventivo a los equipos informáticos?

SI ☐ ***NO*** ☐

15. ¿Se realiza mantenimiento correctivo a los equipos informáticos?

SI ☐ ***NO*** ☐

16. ¿Cuenta con contraseñas para el manejo de la información?

SI ☐ ***NO*** ☐

17. ¿Cuenta con designación de responsabilidades para el cuidado de la información dentro del departamento?

SI ☐ ***NO*** ☐

18. ¿Cuenta con personal de experiencia?

SI ☐ ***NO*** ☐

19. ¿El departamento cuenta con un plan de capacitación para el personal?

SI ☐ ***NO*** ☐

20. ¿Cuentan con licencias del software utilizados para el control y monitoreo que realiza el departamento?

SI ☐ ***NO*** ☐

GRACIAS POR LA ATENCIÓN

Anexo 3

ORDEN DE TRABAJO N° 001

Riobamba, 03 de marzo del 2014

Ing. Edwin Niamiña Lara

DIRECTOR EJECUTIVO DE LA RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO.

De mis consideraciones

Mediante la presente me dirijo a usted para solicitarle de la manera más comedida, autorice la realización de la **AUDITORÍA INFORMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN BAJO LAS NORMAS ISO/IEC 17799, EN LA RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO (REFICH). PERIODO 2012,** la misma que se la desarrollará de acuerdo a las ***NORMASISO/IEC 17799*** emitidas por la Organización Internacional de Estandarización.

Los objetivos de esta Auditoría están encaminados a evaluar del grado de eficiencia y efectividad del sistema de control interno que la Entidad tiene sobre los sistemas informáticos, así como la verificar el cumplimiento de disposiciones legales, reglamentarias y normativas, los resultados se darán a conocer a través del informe de auditoría emitido al final de este trabajo, mismo que incluirá comentarios, conclusiones y recomendaciones.

Atentamente

Ma. Lorena Valle Romero.
SUPERVISOR

Anexo 4

MORALES & VALLE
ASOCIADOS
AUDITORES INDEPENSIENTES CIA. LTDA

Riobamba, 09 de Marzo del 2014

Ing. Edwin Niamiña Lara
DIRECTOR EJECUTIVO DE LA RED DE ESTRUCTURA DE FINANZAS POPULARES Y SOLIDARIAS DE CHIMBORAZO.
Presente.

De mi consideración:

En vista a la autorización que se me ha concedido anteriormente para la realización de una Auditoría Informática a la Seguridad Información para medir el grado de cumplimiento que la Entidad tiene sobre las tecnologías de información, basada en las normas y reglamentos emitidos Organización Internacional de Estandarización (I.S.O) del grupo 17799, me dirijo a Ud. para solicitarle de la manera más comedida su completa colaboración por parte del personal de la Entidad, para acceder a la documentación e información necesaria con la finalidad de poder llevar a cabo la presente investigación solicitada.

Por la atención a la presente reitero mis más sinceros agradecimientos.

Atentamente,

Ma. Lorena Valle Romero
SUPERVISOR