UNIVERSIDAD NACIONAL AUTONOMA DE NICARAGUA, MANAGUA
DEPARTAMENTO DE CONTADURIA PULICA Y FINANZAS.
FACULTAD DE CIENCIAS ECONÓMICAS.
RECINTO UNIVERSITARIO CARLOS FONSECA AMADOR.

Seminario de Graduación para optar al Título de
Licenciado en Contaduría Pública y Finanzas.

Tema: Auditoría Interna.

Sub-tema: Auditoría Interna y Evaluación de Tecnología de la Información, aplicado al Comisariato de la Policía Nacional Masaya en el año 2014.

Integrantes:
Bra. Margarita de los Ángeles Calero Martínez.
Bra. Leylanny Martínez Namoyure.

Tutor: Msc. José Antonio Torres Castro.

Managua, mayo 2015.

Índice

i. Dedicatoria.

A ti mi Dios que has guiado mis caminos llevándome por el mejor de ellos.

A mis hijos Mariana, Benjamín y Camila porque ellos me motivaron a terminar este objetivo que me propuse y siempre han sido

"Cuando las cosas no van como tu esperabas,

No te preocupes, has nuevos planes y recuerda

Que el sol no ha dejado de brillar

Aunque hayan días de tempestad"

Margarita Calero

i. Dedicatoria.

A mi preciosa hija Zohar Camila por ser la luz y motivación; por prestarme tiempo que le pertenecía para poder culminar mi carrera. Este logro nos pertenece.

"Aunque las horas sin mamá
te hayan parecido largas,
y tu llanto interrumpa ni concentración.
Recuerda que mereces una gran madre
Para llegar a ser una gran mujer."

Leylanny Martínez

ii. Agradecimiento.

Le agradezco de todo corazón, primeramente a nuestro Dios padre celestial, quien ha sido siempre mi guía, mi apoyo y sobre todo mi sustento.

A mis padres por haberme apoyado y llenar de esperanza mi futuro y sembrar en mí el deseo de superación.

A mis queridos profesores, que con su labor diaria de enseñanza, apoyo, comprensión y disposición, lograron el triunfo de mi carrera, en especial a mi tutor Msc. José Antonio Torres Castro.

Gracias a todos ellos por haberme permitido llegar hasta donde estoy y lograr ser lo que soy hoy en día.

A mi esposo y mis hijos por darme todo su apoyo, comprensión y motivación para seguir adelante con este objetivo.

Margarita Calero

ii. Agradecimiento.

Nada de lo que vale la pena hacer puede hacerse solo, sino que debe hacerse en colaboración con otros. Por ello deseo expresar mi profundo agradecimiento al grupo de personas cuya orientación y apoyo resultaron imprescindibles para la realización de esta tesis.

Mi eterno agradecimiento a Jehová Dios, por regalarme el tiempo y paciencia y determinación para concluir este seminario.

De manera especial mi agradecimiento a mi Padre José Bayardo Martínez por su confianza depositada en mí y por todas sus muestras de apoyo durante todo este tiempo.

Agradezco a mis compañeros y amigos por su apoyo y especialmente a mi compañera se seminario Margarita Calero por su gran colaboración y trabajo.

Leylanny Martínez.

UNIVERSIDAD NACIONAL AUTONOMA DE NICARAGUA
RECINTO UNIVERSITARIO CARLOS FONSECA AMADOR
FACULTAD DE CIENCIAS ECONOMICAS
DEPARTAMENTO DE CONTADURIA PÚBLICA Y FINANZAS

iii. Valoración del Docente.

Managua, 30 de enero del 2015

Señor
Director
Departamento de Contaduría Pública y Finanzas
Msc. Álvaro Guido Quiroz
Su Despacho.

Estimado Msc. Guido Quiroz:

Tiene la presente la finalidad de informarle que bajo la Modalidad de Culminación de Estudios "Seminario de Graduación", las bachilleras **Margarita de los Ángeles Calero Martínez Carnet** N° **09-209429** y **Leylanny Matilde Martínez Namoyure**, Carnet N°**09-203456**, estudiantes de la Carrera de Contabilidad Pública y Finanzas de la Facultad de Ciencias Económicas de la Universidad Nacional Autónoma de Nicaragua (UNAN), han finalizado de forma satisfactoria su Seminario de Graduación, con el Tema: **Auditoría Interna,** Sub tema: **Auditoria Interna y la Tecnología de la Información: Evaluando la Tecnología de la Información .**

Sin más que agregar.

Atentamente,

Lic. José Antonio Torres Castro.
Tutor- Seminario de Graduación.
Tema Auditoria Interna.

cc: Bachilleres
Archivos

iv. Resumen

En muchas organizaciones la información y la tecnología con la que se cuenta son los activos más importantes y valiosos. En este contexto, El Comisariato de la Policía Nacional de Masaya enfrentan nuevos riesgos que deben ser mitigados a partir del establecimiento de normas respecto a la administración de la Información, a la Tecnología que la soporta, a los ambientes requeridos para la fundación de un área de sistemas, y a la estructura organizacional del área, entre otras.

Además, la empresa debe establecer una estructura de control diseñada de manera tal que contribuya; por una parte, al logro de los objetivos trazados por la organización y, por otra, a la detección de aspectos no previstos que pudieran impedir el logro de dichos objetivos. En ese sentido, los sistemas computarizados tienen el papel de contribuir a alcanzar dichos objetivos.

Las comunicaciones son una de las bases de los negocios modernos, sin las cuales ninguna empresa podría sobrevivir. Por eso la auditoría en Tecnología de la Información cobra cada vez más relevancia, tanto a nivel nacional como internacional; debido a las constantes vulnerabilidades que se encuentran en las redes.

La Auditoría de Tecnología de la Información es un análisis orientado a proporcionar información y recomendaciones que les permite a la empresa determinar las acciones necesarias para crecer y alcanzar un nivel de rendimiento y disponibilidad de la red, acorde a las necesidades actuales y futuras del negocio; sin comprometer la seguridad empresarial.

I. Introducción.

El crecimiento acelerado que se han producido en las empresas en el campo tecnológico ha demandado mejores prácticas de administración de los equipos y del personal técnico a cargo. Dicho crecimiento también genera un cambio operacional y financiero, ha significado también una expansión en su cobertura, productos y servicios mediante el uso de la tecnología y los sistemas de información.

Dicho uso creciente de la tecnología de información conlleva también una mayor dependencia hacia ella y por lo tanto, los riesgos relacionados a la tecnología de información se transfieren a los procesos del negocio; lo cual, involucra una responsabilidad para la Alta Dirección respecto a la administración de los riesgos relacionados con la tecnología de información ya que el no hacerlo podría poner en riesgo la seguridad de uno de sus activos más importantes: la información; y, la continuidad de sus operaciones, acarreando incuantificables pérdidas financieras y hasta la desaparición de la Entidad.

Es por ello, que tanto organizaciones internacionales como gubernamentales han emitido una serie de normas, estándares y mejores prácticas como: COSO, COBIT, ISO etc. que permitan a las Entidades Financieras y comerciales poder hacer frente al desafío de lograr una adecuada administración de los procesos, las personas, la tecnología y los eventos externos en forma efectiva y sustentable, bajo un adecuado ambiente de control interno.

Por consiguiente, para el éxito dentro de la administración del riesgo tecnológico es necesario el liderazgo de la Alta Dirección y el compromiso de todos quienes conforman la Entidad hacia una cultura de control interno y prevención del riesgo, basado en los diferentes lineamientos, marcos de referencia, estándares y regulaciones vigentes, adaptado a las necesidades y requerimientos de cada Entidad, buscando la seguridad de la información y la continuidad del negocio enforna sustentable; de tal manera, que se agregue valor y ventaja competitiva a las operaciones que realizan.

Es necesario que se diseñen, implementen y mejoren una metodología para la administración del riesgo operativo, considerando en forma especial el factor de la tecnología con la finalidad de garantizar la seguridad de la información y la continuidad de las operaciones, conscientes de la importancia que tiene la tecnología de información y el control interno dentro de la cadena de valor del negocio y en la estructura organizacional que la conforma.

El presente seminario busca establecer un marco de control relacionado con la tecnología de información que sirva de guía para Directivos, Gerentes de TI, Auditores en el comisariato de la Policía nacional de Masaya tomando en consideración que se busca proteger los recursos financieros de los socios que han puesto su confianza endicho sector financiero.

Estructura del Seminario

En el capítulo 4.1 (Según índice) se expone los antecedentes y definiciones sobre la Auditoria Interna. Como se desarrolla, sus aplicaciones y exigencia para las buenas practicas del auditor interno.

El capítulo 4.2 indica el modelo COBIT, el cual es usado para este trabajo; describiendo los productos Cobit 4.0, sus generalidades, sus respectivos dominios y las ventajas sobre otros modelos.

En el **Capítulo 4.3** describimos a la empresa (Donde se aplicó la auditoria) su entorno y situación actual. Estructura orgánica y personal disponible a ser auditado.

En el **Capítulo 4.4** exponemos los pasos para elaborar la auditoria interna en el área informática, compuesta de: Plan de trabajo, distribución del personal participante, cronograma de trabajo, etc. Además de las entrevistas y papeles de trabajos desarrollados durante la auditoria interna para llegar a las conclusiones y resultados. Al **final** del presente trabajo se exponen las **conclusiones** de la investigación, el grado de cumplimiento de objetivos y validación de hipótesis, así como recomendaciones y vetas para futuras posibles investigaciones, los anexos y la bibliografía utilizada.

II. Justificación.

La realidad actual exige la incorporación de elementos que faciliten la actividad gerencial, a fin de mejorar el desempeño profesional, como herramientas para un acceso rápido a la información. Desde el punto de vista de las funciones gerenciales, la tecnología de la información contribuye a optimizar el proceso administrativo, facilitando la celeridad y ahorro de tiempo en la expedición de documentos, notas y cualquier otro servicio que se requiera.

De igual forma el uso de la tecnología de la información resultará beneficioso para los hechos pedagógicos porque su hábil guía será aprovechado en la obtención de conocimientos referidos al aspecto formativo. Siendo este aspecto el que sirva de base para justificar esta investigación, tomando en cuenta que la formación del gerente en el uso y manejo de la tecnología de la información.

El análisis de los objetivos de control con el COBIT4.0, debe ser de carácter objetivo e independiente, critico , basado en evidencias , sistemático bajo normas y metodologías aprobadas a nivel internacional, que seleccione políticas, normas prácticas, funciones y procesos que permitan obtener una opinión profesional e imparcial.

La situación actual por la que atraviesa el área de informática del Comisariato de la Policía Nacional de Masaya requiere que mediante de procedimientos y técnicas, se proceda a evaluar y controlar los posibles problemas como:

- Desconocimiento en el nivel directivo de la situación informática de la empresa
- Falta total o parcial de seguridades lógicas y físicas que garanticen la integridad del personal, equipos e información.
- Falta de una planificación informática
- Organización que no funciona correctamente, falta de políticas, objetivos, normas, metodología, asignación de tareas y adecuada administración del Recurso Humano
- Falta de documentación o documentación incompleta de sistemas que revela la dificultad de efectuar el mantenimiento de los sistemas en producción.

III. Objetivos.

3.1 **Objetivo General:**

Desarrollar una auditoría interna de la tecnología de la información (Informática) en la empresa del comisariato de la Policía Nacional Masaya; aplicando las técnicas y procedimientos del Cobit 4.0, a fin de evaluar los principales riesgos tecnológicos a que se enfrenta la empresa, la manera de administrativos y controlarlos para un adecuado funcionamiento de las operaciones.

2.2 Objetivos específicos:

- Analizar el marco conceptual, las aplicaciones y procedimientos de la auditoría interna y tecnología de la información, con el objeto que sea fundamento para el desarrollo de nuestra auditoria.

- Aplicar el estándar Cobit 4.0 en la evaluación y auditoría interna del Comisariato de la Policía Nacional Masaya

- Emitir recomendaciones que permitan asegurar una mayor integridad, confidencialidad y confiabilidad de la información en base a la auditoría realizada, en el comisariato de la Policía Nacional de Masaya

IV. Auditoría Interna.

Actualmente las empresas han alcanzado un nivel mayor de desarrollo, muchas veces sujetas a la complejidad de sus operaciones y otros factores externos por lo que se ven en la necesidad de contar con los servicios de la unidad de auditoría interna, ya que ésta les proporciona mayor seguridad en sus activos y un mayor logro de metas y objetivos.

Por lo tanto, los profesionales de auditoría interna están obligados a contar con la adecuada preparación y capacidad profesional para proporcionar un servicio de calidad y valor agregado a las empresas. También podemos definirla como un proceso sistemático, practicado por los auditores de conformidad con normas y procedimientos técnicos establecidos, consistente en obtener y evaluar objetivamente las evidencias sobre las afirmaciones contenidas en los actos jurídicos o eventos de carácter técnico, económico, administrativo y otros, con el fin de determinar el grado de correspondencia entre esas afirmaciones, las disposiciones legales vigentes y los criterios establecidos.

4.1 Antecedentes de la auditoría interna.

Las primeras referencias de auditoría eran muy sencillas pero fue hasta el siglo XIX las funciones principales de la auditoría estaban encaminadas a la prevención, divulgación y castigo del fraude y del engaño, debido a que su enfoque era solamente empírico, y no existía ninguna actitud, normatividad ni disciplina profesional que la regulara. A su vez el desarrollo del comercio, trajo consigo la necesidad de las revisiones independientes para asegurarse de la adecuación y finalidad de los registros mantenidos en las empresas.

La auditoría como profesión fue reconocida por primera vez bajo la Ley Británica de Sociedades Anónimas de 1862. Desde 1862 hasta 1905 la profesión de la Auditoría creció y floreció en Inglaterra. En 1900, la Auditoría se introdujo en los Estados Unidos, cuyo objetivo principal consistía en la revisión de los estados financieros y de los resultados de las operaciones. Solo a partir de ese momento se desarrolla el modelo de Auditoría Interna y de Gobierno, lo que permitió que la Auditoría se convirtiera en un proceso integral y de asesoría al interior de las empresas, afianzando la creación de un Sistema de Control para cada una de ellas. (Bacón, Charles A., manual de Auditoría Interna pág.1, segunda edición)

En 1941, con el nacimiento del Instituto de Auditores Internos (IIA) de Nueva York se llegó a la conclusión de buscar e informar sobre irregularidades y fraude no era la mayor responsabilidad de los auditores externos, convirtiéndose en responsabilidad de los auditores internos.

En el año de 1947, el Instituto en referencia emitió el cuadro de responsabilidades de la auditoría interna, el cual es sometido a revisiones periódicas, siendo estas realizadas durante los años de 1957, 1971 y la última efectuada en el año de 1981. (Santillana González, Juan Ramón, conoce las auditorías pàg.115)

Y como parte del compromiso adquirido con los profesionales de auditoría interna, el Instituto en mención, creó y adoptó en 1968 el Código de Ética del auditor interno. Este documento entre, otras cosas, regula el comportamiento que debe observar el auditor interno. Años más tarde en 1974 es creado un comité de Normas y Responsabilidades profesionales, el cual se encarga de la elaboración y promulgación de las Normas para el Ejercicio Profesional de la Auditoría Interna (NEPAI), acontecimiento que ha contribuido enormemente al reconocimiento de la auditoría interna y colocarla en un lugar de importancia dentro de las entidades.

4.1.2 Definición de auditoría interna.

En junio de 1999, la Junta Directiva del IIA aprobó la siguiente Definición de la

Auditoría Interna:

“La auditoría interna es una actividad de evaluación independiente y objetiva de aseguramiento y consulta, cuya finalidad es aumentar el valor y mejorar las operaciones de la organización. Ayuda a que la organización cumpla con sus objetivos mediante la aplicación de un enfoque sistemático y disciplinado para evaluar y mejorar la efectividad de los procesos de manejo de riesgos, control y dirección”.

Se puede decir que la auditoría interna se constituye en una función de asesoría, que proporciona seguridad para la empresa en el manejo de las operaciones, ya que evalúa en forma permanente el adecuado funcionamiento de los controles internos establecidos. Al

mismo tiempo examina el grado de cumplimiento de los objetivos, principalmente aquellos orientados a la implementación de medidas preventivas y/o correctivas.

4.1.3 Características de la auditoría interna.

La auditoría interna tiene sus propias características básicas y su campo de acción, debido a las diferentes actividades económicas y financieras.

Las principales características básicas a mencionar son las siguientes:

- Auditoría tradicional o financiera
- Verifica eventos pasados
- Examina la actividad económica
- Comprueba los eventos financieros
- Dependencia de la Gerencia General o Junta Directiva
- Reporta e informa de quien depende
- Independencia respecto a las partes auditadas
- Independencia mental (no económica).

4.1.4 Objetivo y alcances de la auditoría interna.

El objetivo de la auditoría interna es prestar un servicio de asistencia constructiva a la administración, con el propósito de mejorar la conducción de las operaciones y de obtener un mayor beneficio económico para la empresa, tomando en consideración el cumplimiento de las normas para el ejercicio profesional de la auditoría interna y las declaraciones sobre normas de auditoría interna. Con este fin les proporciona análisis, valoraciones, recomendaciones, consejos e información concerniente a las actividades revisadas.

El auditor interno al finalizar su examen, ha de informar a la administración, con objetividad profesional y absoluta independencia de criterio, el resultado final de su trabajo, expuesto en forma de análisis, evaluaciones, observaciones y comentarios, así como sus conclusiones y recomendaciones.

El alcance comprende el examen y valoración de lo adecuado y efectivo de los sistemas de control interno de una organización, y de la calidad de la ejecución al llevar a cabo las responsabilidades asignadas.

4.1.5 Funciones de la auditoría interna.

El entorno económico, político y social genera cambios en los sistemas de control interno en las empresas, ya que los riesgos varían, las necesidades son otras, las culturas se transforman y los avances tecnológicos son vertiginosos, la implementación y evaluación de los controles, no pueden ser responsabilidad aislada de la administración, lo que conlleva a la unidad de auditoría interna a que sus funciones se adapten a las necesidades que exigen las actuales tendencias de las empresas. (Disponible en biblioteca.utec.edu.sv, Universidad tecnológica de El Salvador, 2009).

Por lo que se determinan como principales funciones las siguientes:

- Evaluar en forma permanente, el funcionamiento de los controles internos establecidos por la Administración y recomendar las medidas que signifiquen mejorar su efectividad.
- Examinar el grado de cumplimiento de los objetivos y políticas, así como, las metas de corto, mediano y largo plazo, para cumplir este propósito, es fundamental que las áreas de control se encuentren claramente establecidas, con la existencia de un sistema de información confiable, que permita conocer oportunamente los avances y ejecuciones.
- Evaluar, cualitativa y cuantitativamente, los medios y formas de generación de información para el proceso de toma de decisiones.
- Determinar el grado de economía y eficiencia con que se utilizan los recursos de la entidad, considerando aspectos técnicos, criterios económicos, sociales y culturales existentes.

4.1.6 Rol del Auditor interno.

El auditor en su rol de trabajo continuo realiza las siguientes funciones. Claro estas puedes ser variables dependiendo en el área que se desarrolle. Algunos de los roles desempeñados generalmente son los siguientes:

- **Evalúa en forma directa los controles internos** y formula recomendaciones para su optimización

- **Revisa la fiabilidad e integridad de la información** financiera y operativa y de los procedimientos aplicados en la organización **Revisa los sistemas establecidos** con el fin de asegurar el **cumplimento** de las políticas, planes, procedimientos, leyes y otros que afecten las operaciones de la organización

- **Analiza las operaciones** para verificar si los resultados son coherentes con los objetivos y metas previamente establecidas (eficiencia, eficacia y economía en el uso de los recursos) **(citado por Raúl Pineda, Medellín Sept. 2012)**

Donde el auditor interno tiene que comprender y aplicar las mejores prácticas, procesos tecnológicos, evaluar los controles y la gobernabilidad, todo esto es parte de la tendencia actual en la auditoría interna.

Consideremos que un auditor interno puede convertirse en los ojos y oídos de la dirección de la empresa, teniendo en cuenta, no solo su calificación y ética moral, sino porque se trata de un funcionario que con el tiempo logra obtener un alto dominio de todas y cada una de sus funciones de la empresa donde labora, lo que le permite convertirse en un asesor o de los ejecutivos de la gestión empresarial.

4.1.7 Perfil profesional del auditor interno

El concepto tradicionalmente policial del auditor interno ha evolucionado a través del tiempo. La nueva concepción tiende a considerar a la auditoría interna más bien como un servicio de asistencia técnica al personal, dentro de las empresas, sin descuidar su primordial responsabilidad de revisar las operaciones y evaluar el funcionamiento del control interno.

El moderno auditor interno no es el simple revisor de cuentas de otros tiempos, en la actualidad tanto la alta dirección de la empresa como sus ejecutivos superiores, confían no sólo en la habilidad profesional del auditor interno en cuanto a poner de manifiesto errores y deficiencias, sino en su buen juicio para sugerir fórmulas eficaces para la solución de problemas.

El auditor interno es por su formación profesional y conocimiento integral de la institución uno de los hombres más calificados para ayudar al desarrollo tanto del recurso humano como de mejorar las diferentes operaciones.

En la actualidad se demanda de un profesional de auditoría interna con un perfil como el siguiente:

Áreas	Conocimientos	Habilidades	Actitudes y Valores
Personal	Administración de Desarrollo gerencial Idioma ingles Técnicas motivacionales Normas y Procedimientos de auditoría	Liderazgo Capacidad de análisis y Trabajo de equipo Disciplinado Crítico y visionarios Toma de decisiones Comunicativo Expresión oral y escrita Dinámico Creativo	Honrado Responsable Iniciativa Organizado Independencia mental Ético Humanitario Fidedigno Participativo Educación Continuada
Especialidades	Auditoria y contabilidad Planeación estratégica Legislación mercantil, tributaria y laboral Finanzas Consultoría financiera y fiscal	Uso de software: Uso de equipo de Oficina. Diseño de sistemas de)etección de fraudes. Servicio al cliente Estratégico Dominio de cifras y datos.	Puntualidad Investigador Motivador Imparcial Amplitud de criterio Eficaz y eficiente

Fuente: Auditoria Interna Moderna, 2010, pág. 125. Edición 3ra.

4.1.8 Requisitos para ser Auditor Interno y su certificación en Nicaragua.

Actualmente para poder ser Auditor interno certificado en la República de Nicaragua, se necesitan una serie de requisitos, para dar fe que están calificados para desempeñar esta

función. Los CIA´S (Certifiedinternal auditor) tienen la única designación profesional internacional que existe para los auditores internos, los auditores que se certifican incrementan su valor para la dirección superior de la empresa ya que demuestran ser auditores competentes y realzan su imagen profesional. El título de reconocimiento lo entrega TheInstitute of InternalAuditors.

Ciertos requisitos son los siguientes:

- Obtener el título universitario de Licenciado en Contaduría pública.
- Tener al menos dos años de experiencia en auditoría interna o bien un grado de maestría.
- Obtener la autorización del sitio oficial para el examen en el mes de noviembre
- Presentar al Instituto internacional de Auditores la documentación pertinente para que autorice la dispensa de la parte IV.
- Pedir al supervisor, gerente u otro auditor interno un certificado que complete un formulario de referencia que acredite tus altos valores morales y tus comportamientos éticos en los negocios.
- La experiencia en auditoría interna o externa de un candidato debe hacer constar en papel membretado de su empresa e indicar las fechas específicas de su empleo, funciones de auditoría y ser firmado por el jefe inmediato o gerente de auditoría.
- Ejecutar un programa de entrenamiento con base al Mini Gleim.
- Desarrollar un programa de entrenamiento en conjunto con la asociación de auditores internos de Nicaragua y el colegio de contadores públicos de Nicaragua
- Aplica y registrarse para el examen de la CIA (certifiedinternal auditor). La solicitud y el formulario están disponibles en la Asociación de auditores internos de Nicaragua. Este título se obtiene aprobando un examen de dos días que se toma en los meses de mayo y noviembre. El examen se toma por computadora y se evalúan cuatro partes:

- Parte I: El papel de la auditoría interna en el gobierno corporativo, el riesgo y el control.
- Parte II: Realización del trabajo de auditoría interna
- Parte III: Análisis de empresas y tecnología informática.
- Parte IV: Habilidades para la administración de empresas.

Durante el proceso de solicitud, es necesario proporcionar comprobantes del título de licenciatura y de la experiencia en auditoría interna así como también el formulario de referencias.

Los CIA´S (certifiedinternal auditor) tienen la única designación profesional internacional que existe para los auditores internos, los auditores que se certifican incrementan su valor para la dirección superior de la empresa ya que demuestran ser auditores competentes y realzan su imagen profesional. El título de reconocimiento lo entrega TheInstitute of InternalAuditors.

4.1.9 Tipos de auditoría interna

La auditoría interna tiene los objetivos y funciones ya indicados en el apartado anterior, eso quiere decir que surge la necesidad de la especialización en la evaluación del control interno.

Se pueden diferenciar en este sentido auditorías que pueden considerarse como:

- Auditoria operativa o de gestión: Es la valoración independiente de todas las operaciones de una empresa, en forma analítica objetiva y sistemática, para determinar si se llevan a cabo, políticas y procedimientos aceptables; si se siguen las normas establecidas, si se utilizan los recursos de forma eficaz y económica y si los objetivos de la organización se han alcanzado para así maximizar resultados que fortalezcan el desarrollo de la empresa.

- Auditoria de calidad: En este tipo de auditoría podemos hablar de aquellas auditorías de calidad destinadas a salvaguardar que se cumplan las normas ISO.

- Auditoría administrativa: Una auditoria administrativa es la revisión analítica total o parcial de una organización con el propósito de precisar su nivel de desempeño y

perfilar oportunidades de mejora para innovar valor y lograr una ventaja competitiva sustentable.

- Auditoria informática: consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas.

- Auditoría fiscal o tributaria: es un procedimiento, basado en la normativa legal y administrativa vigente, destinado a fiscalizar el correcto cumplimiento de la obligación tributaria de los contribuyentes.

4.1.10 Ventajas de la auditoría interna.

Algunas de las ventajas de seguir con los lineamientos de la auditoria interna son los siguientes:

- Facilita una ayuda primordial a la dirección al evaluar de forma relativamente independiente los sistemas de organización y de administración.

- Realiza una evaluación global y objetiva de los problemas de la empresa, que generalmente suelen ser interpretados de una manera parcial por los departamentos afectados.

- Pone a disposición de la dirección un profundo conocimiento de las operaciones de la empresa, proporcionado por el trabajo de verificación de los datos contables y financieros.

- Contribuye eficazmente a evitar las actividades rutinarias y la inercia burocrática que generalmente se desarrollan en las grandes empresas.

- Favorece la protección de los intereses y bienes de la empresa frente a terceros.

- Actúa como un elemento del aseguramiento corporativo.

4.1.11 Normas para el ejercicio profesional de la auditoría interna (NEPAI).

"Las Normas de Auditoría Interna son las formalidades indispensables que guardan relación con la independencia de la unidad, la integridad y capacidad profesional del auditor interno, el proceso de su trabajo y con la dirección de la unidad a su cargo ". (Asociación de Auditores Internos de El Salvador (AUDISAL), 2009)

Las Normas para el Ejercicio Profesional son paralelas al proceso de auditoría interna y establecen el criterio de calidad para evaluar el ejercicio de la profesión.

Esta presentación cumple con el marco de prácticas profesionales aprobado por la junta directiva del IIA en junio de 1999.

El Instituto de Auditores Internos (IIA), es el organismo que se ha venido preocupando por el desarrollo profesional de la auditoría interna y como resultado de ello, en la década de los setenta se crean las Normas para el Ejercicio Profesional de la Auditoría Interna (NIEPAI).

Los objetivos de las normas de auditoría interna son:

- Divulgar como debe entenderse la gestión de auditoría interna.
- Difundir las responsabilidades de la auditoría interna.
- Enmarcar los principios que orientan la actividad de la auditoría interna
- Evaluar el funcionamiento de la unidad de auditoría interna.
- Mejorar los conocimientos de auditoría interna.

La importancia de las normas de auditoría interna radica en que dichas normas tienen como objetivo principal indicar como debe practicarse la auditoría interna.

Durante la IV convención nacional de Contadores públicos celebrada en julio de 1996, retornando el esfuerzo realizado por auditoría interna, se recomendó la adopción de las normas para el ejercicio profesional de auditoría interna (NIEPAI), emitidas por el Instituto de Auditores Internos (IIA), con la salvedad de no adoptar aquellos aspectos no aplicables en el medio .

El propósito de las normas es:

- Definir principios básicos que representen el ejercicio de la auditoría interna tal como este debería ser.
- Proveer un marco para ejercer y promover un amplio rango de actividades de auditoría interna de valor agregado.
- Establecer las bases para medir el desempeño de la auditoría interna.
- Fomentar la mejora en los procesos y operaciones de las empresas.

Las Normas se dividen en:

- **Normas sobre atributos:** Tratan sobre las características de las entidades y los individuos que desarrollan actividades de auditoría interna
- **Normas sobre desempeño:** Describen la naturaleza de las actividades de auditoría interna y proveen criterio de calidad contra los cuales puede medirse la práctica de estos servicios.
- **Normas de Implementación**: Estas son aplicables a tipos específicos de trabajo.
- **Normas de sobre atributos y sobre desempeños:** Se aplica a todos los servicios de auditoría interna en general.

La relación de las NIA's con las NIEPAI es que ambas normas están orientadas llevar a cabo una auditoría en forma eficiente, a través de una adecuada planificación y ejecución, evaluando adecuadamente los controles internos existente que contribuyen a determinar el alcance de los procedimientos de auditoría.

4.1.12 Comité de Auditoría.

El Comité de Auditoría es un órgano dentro del gobierno corporativo que normalmente es utilizado en organizaciones con un tamaño representativo.

Este sirve de enlace entre la Junta Directiva, Auditoría Interna, Auditoría Externa y otros órganos de control dentro de la organización. En la actualidad el Comité de Auditoría se ha convertido en una herramienta indispensable en las grandes organizaciones a nivel mundial, tanto así que se puede ubicar el mismo en el 95% de las corporaciones. En nuestro entorno centroamericano resulta común que organizaciones de un tamaño considerable, ya sea en el

sector privado o público, no cuenten con un Comité de Auditoría, esto ocurre en algunos casos porque no se tiene claro sobre las bondades que proporciona su implementación.

La conformación de los miembros que integran un Comité de Auditoría debe ser realizada por la Junta Directiva. Los miembros de este Comité normalmente son integrantes de la Junta Directiva pero en algunos casos ocurre que se integran miembros externos a esta. No es aconsejable que el Comité de Auditoría esté integrado por miembros que formen parte de la administración, ni por el Presidente de la Junta Directiva. Las mejores prácticas establecen que cinco miembros es la cantidad ideal con la que deben contar estos Comités.

El Comité de Auditoría debe servir como el eje que distribuya de manera adecuada los recursos de auditoría de los que dispone la administración, de manera que asignen de manera adecuada los alcances en los estudios que realizan tanto los auditores externos como los auditores internos y no se dupliquen estas labores.

Debe existir entre el Comité de Auditoría y la Auditoría Interna una relación cercana, en la que ambos sean interdependientes y mutuamente accesibles, ya que por ejemplo el Comité de Auditoría debe evaluar el Plan Anual de Trabajo de la Auditoría Interna, el estatuto de la Auditoría Interna, los informes y los principales hallazgos. También debe comprobar que la Auditoría incluya dentro de su Plan anual de Trabajo, la evaluación del cumplimiento con leyes, ética, regulaciones, temas de gobierno corporativo y sus riesgos relacionados.

Asimismo debe coordinar la ejecución del Programa de Aseguramiento de la Calidad realizada al departamento de Auditoría Interna, tanto en sus evaluaciones internas (Autoevaluaciones) como en sus evaluaciones externas, esto para verificar la calidad con la que desarrolla sus funciones la Auditoría Interna.

Con respecto a temas de gobierno y administración dentro de la organización, el Comité de Auditoría debe realizar lo siguiente:

- Comprobación de que exista un proceso continuo de administración de riesgos eficaz y un marco de referencia para evaluación de riesgos implementado en la organización (COSO, Basilea, entre otros).

- Evaluar el compromiso con un adecuado control interno a lo largo de toda la organización y emanado desde la alta gerencia.

- Evaluación de políticas corporativas relacionadas con cumplimiento de leyes, regulaciones, ética, conflictos de interés, fraude e investigaciones de conductas inapropiadas.

- Revisión del cumplimiento con temas de gobierno corporativo.

- Con respecto al Código de Ética: revisar que esté establecido el mismo dentro de la organización, que haya sido comunicado a todos los miembros de la organización, evaluar que esté actualizado y analizar de manera periódica el reporte de incumplimientos con el mismo.

- Revisión del plan de la administración para evaluar cumplimiento con la ética, regulaciones, leyes, temas de gobierno corporativo, entre otros.

- Identificación de tendencias negativas y positivas y revisión de planes de la administración para darle un tratamiento a las mismas.

- Mantenerse informados sobre los principales temas de la organización, investigaciones y acciones disciplinarias.

- Comunicación permanente con alta gerencia sobre nuevos procesos, áreas problemáticas, avances en temas importantes, entre otros.

- Verificación de que exista un programa antifraude y que se le dé un seguimiento adecuado al mismo. (Revista Zona Centro, edición 53, mayo 2011, pág. 52-53).

4.1.13 Gobierno de la Auditoría Interna.

Y que conforme las Normas se considera Gobierno a la "La combinación de procesos y estructuras implantados por el Consejo de Administración para informar, dirigir, gestionar y vigilar las actividades de la organización con el fin de lograr sus objetivos".

El término Consejo (Consejo de Administración) se refiere al cuerpo de gobierno de una organización, tal como el consejo de administración, el consejo de supervisión, el responsable de un organismo o cuerpo legislativo, el comité o miembros de la dirección de una organización sin ánimo de lucro, o cualquier otro órgano de gobierno designado por la organización, a quien pueda reportar funcionalmente el director ejecutivo de auditoría.

Respecto a las Normas sobre Desempeño, las siguientes Normas tienen relación con Gobierno:

2110 Gobierno: La actividad de auditoría interna debe evaluar y hacer las recomendaciones apropiadas para mejorar el proceso de gobierno en el cumplimiento de los siguientes objetivos:

- Promover la ética y los valores apropiados dentro de la organización.
- Asegurar la gestión y responsabilidad eficaces en el desempeño de la organización.
- Comunicar la información de riesgo y control a las áreas adecuadas de la organización.
- Coordinar las actividades y la información de comunicación entre el Consejo de Administración, los auditores internos y externos, y la dirección.

2110. A1 La actividad de auditoría interna debe evaluar el diseño, implantación y eficacia de los objetivos, programas y actividades de la organización relacionados con la ética.

2110. A2 La actividad de auditoría interna debe evaluar si el gobierno de tecnología de la información de la organización apoya las estrategias y objetivos de la organización.

Gobierno de tecnología de la información - Consiste en el liderazgo, las estructuras de la organización y los procesos que aseguran que la tecnología de la información de la empresa soporta las estrategias y objetivos de la organización.

Controles de tecnología de la información - Controles que soportan la gestión y el gobierno del negocio, y proporcionan controles generales y técnicos sobre las infraestructuras de tecnología de la información tales como aplicaciones, información, infraestructura y personas. (Publicación N° 4 - FELABAN - código marco de prácticas de buen gobierno corporativo para entidades del sector financiero latinoamericano – 2009).

4.2 Tecnología de la información y COBIT.

4.2.1 Que son las tecnologías de Información.

La tecnología de información (TI) según lo definido por la asociación de la tecnología de información de América (por sus siglas en Ingles ITAA) es “el estudio, diseño, desarrollo, implementación, soporte o dirección de los sistemas de información computarizados, en particular de software de aplicación y hardware de computadoras.” Se ocupa del uso de las computadoras y su software para convertir, almacenar, proteger, procesar, transmitir y recuperar la información.

Hoy en día, el término “tecnología de información” se suele mezclar con muchos aspectos de la computación y la tecnología y el término es más reconocible que antes.

La tecnología de la información puede ser bastante amplia, cubriendo muchos campos. Los profesionales TI realizan una variedad de tareas que van desde instalar aplicaciones a diseñar complejas redes de computación y bases de datos.

Algunas de las tareas de los profesionales TI incluyen, administración de datos, redes, ingeniería de hardware, diseño de programas y bases de datos, así como la administración y dirección de los sistemas completos. Cuando las tecnologías de computación y comunicación se combinan, el resultado es la tecnología de la información o “infotech”. La Tecnología de la Información (TI) es un término general que describe cualquier tecnología que ayuda a producir, manipular, almacenar, comunicar, y/o esparcir información.

4.2.2 Tipos de tecnologías de información (TI).

El término “tecnología de información” se ha expandido para abarcar muchos aspectos de computadora y de la tecnología, este es más reconocible que antes. El mundo de la tecnología de información puede ser absolutamente grande, cubriendo muchos campos.

Los profesionales realizan una variedad de deberes que se extienden desde instalar aplicaciones, a diseñar redes de ordenadores y bases de datos complejas de la información. Algunos de los deberes que los profesionales realizan pueden incluir:

- Gerencia de datos
- Establecimiento de una red de la computadora
- Diseño de los sistemas de la base de datos
- Diseño del software
- Sistemas de información de gerencia
- Gerencia de sistemas

4.2.3 Auditoría en tecnologías de la información.

Una auditoría a tecnologías de la información es un examen profesional, objetivo y sistemático de las operaciones y actividades efectuadas por una organización, proyecto o programa, para determinar el grado de cumplimiento y eficacia de:

- La planificación, el desarrollo y la implantación de los sistemas utilizados.
- La información producida por los sistemas, su pertinencia y confiabilidad.
- La documentación básica de cada sistema, su implantación y la divulgación de la misma entre los usuarios.
- Los mecanismos de control incorporados en los sistemas.

- Los recursos idóneos identificados y disponibles para garantizar la continuidad de las operaciones en caso de desastres.

- El programa de adiestramiento al personal de sistemas de información, sus usuarios y los auditores.

Entonces, se entiende por auditoría a tecnologías de la información a aquella actividad auditora que trata de evaluar la adecuada utilidad, eficiencia y fiabilidad de la información mecanizada que se produce en una determinada empresa o institución, así como la organización de los servicios que la elaboran y procesan.

Por lo tanto la auditoría a tecnologías de la información debe analizar la función informática, que engloba el análisis de la organización, seguridad, segregación de funciones y gestión de las actividades de proceso de datos.

4.2.4 Objetivos de una Auditoría en tecnologías de la información.

La Auditoria de Tecnología de la Información tiene como objetivos los siguientes.

- Verificar el control de la función informática, asegurando 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 traspasos de fondos.

- Buscar una mejor relación costo-beneficio de los sistemas automáticos o informáticos.

- Asegurar una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles.

- Conocer la situación actual del área informática y las actividades y esfuerzos necesarios para lograr los objetivos propuestos.
- Seguridad de personal, datos, hardware, software e instalaciones.
- Seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático.
- Minimizar existencias de riesgos en el uso de tecnología de información.
- Decisiones de inversión y gastos innecesarios.
- Capacitación y educación sobre controles en los sistemas de información.

4.2.5 Introducción - Modelo COBIT.

La Misión de COBIT: Investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes de empresas y auditores.

COBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información (IT). - **COBIT es *la* herramienta innovadora para el gobierno de IT** -.

COBIT se fundamenta en los Objetivos de Control existentes de la *InformationSystemsAudit and Control Foundation*(ISACF), mejorados a partir de estándares internacionales técnicos, profesionales, regulatorios y específicos para la industria, tanto existentes como en surgimiento. Los Objetivos de Control resultantes han sido desarrollados para su aplicación en **sistemas de información en toda la empresa**. El término **"generalmente aplicable y aceptado"** es utilizado explícitamente en el mismo sentido que los Principios de Contabilidad Generalmente Aceptados (PCGA o GAAP por sus siglas en inglés). Para propósitos del proyecto, **"buenas prácticas"** significa consenso por parte de los expertos.

Este estándar es relativamente pequeño en tamaño, con el fin de ser práctico y responder, en la medida de lo posible, a las necesidades de negocio, manteniendo al mismo tiempo una independencia con respecto a las plataformas técnicas de IT adoptadas en una organización.

El proporcionar indicadores de desempeño (normas, reglas, etc.), ha sido identificado como prioridad para las mejoras futuras que se realizarán al marco referencial.

El desarrollo de *COBIT* ha traído como resultado la publicación del Marco Referencial general y de los Objetivos de Control detallados, y le seguirán actividades educativas. Estas actividades asegurarán el uso general de los resultados del Proyecto de Investigación COBIT.

4.2.6 Contenido (Productos Cobit).

El desarrollo de COBIT ha resultado en la publicación de:

• un ***Resumen Ejecutivo*** el cual, adicionalmente a esta sección de antecedentes, consiste en un Síntesis Ejecutiva (que proporciona a la alta gerencia entendimiento y conciencia sobre los conceptos clave y principios de COBIT) y el *Marco Referencial* (el cual proporciona a la alta gerencia un entendimiento más detallado de los conceptos clave y principios de COBIT e identifica los cuatro dominios de COBIT y los correspondientes 34 procesos de IT).

• el ***Marco Referencial*** que describe en detalle los 34 objetivos de control de alto nivel e identifica los requerimientos de negocio para la información y los recursos de IT que son impactados en forma primaria por cada objetivo de control.

• ***Objetivos de Control***, los cuales contienen declaraciones de los resultados deseados o propósitos a ser alcanzados mediante la implementación de 302 objetivos de control detallado y específico a través de los 34 procesos de IT.

• ***Guías de Auditoría***, las cuales contienen los pasos de auditoría correspondientes a cada uno de los 34 objetivos de control de IT de alto nivel para proporcionar asistencia a los auditores de sistemas en la revisión de los procesos de IT con respecto a los 302 objetivos detallados de control recomendados para proporcionar a la gerencia certeza o recomendaciones de mejoramiento.

• Un ***Conjunto de Herramientas de Implementación***, el cual proporciona lecciones aprendidas por organizaciones que han aplicado COBIT rápida y exitosamente en sus ambientes de trabajo.

El Conjunto de Herramientas de Implementación incluye la *Síntesis Ejecutiva*, proporcionando a la alta gerencia conciencia y entendimiento de COBIT. También incluye una guía de implementación con dos útiles herramientas - Diagnóstico de la Conciencia de la Gerencia4 y el Diagnóstico de Control de TI5 - para proporcionar asistencia en el análisis del ambiente de control en IT de una organización. También se incluyen varios casos de estudio que detallan como organizaciones en todo el mundo han implementado COBIT exitosamente. Adicionalmente, se incluyen respuestas a las 25 preguntas más frecuentes acerca de COBIT y varias presentaciones para distintos niveles jerárquicos y audiencias dentro de las organizaciones.

4.2.7 Alcance y Resumen Ejecutivo COBIT.

COBIT evolucionará a través de los años y será el fundamento de investigaciones futuras. Por lo tanto, se generará una familia de productos COBIT y al ocurrir esto, las tareas y actividades que sirven como la estructura para organizar los Objetivos de Control de IT, serán refinadas posteriormente, también será revisado el balance entre los dominios y los procesos a la luz de los cambios en la industria.

4.2.8 Resumen Ejecutivo del COBIT.

Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la Tecnología de Información (IT) relacionada. En esta sociedad global (donde la información viaja a través del "ciberespacio" sin las restricciones de tiempo, distancia y velocidad) esta criticalidad emerge de:

• La creciente dependencia en información y en los sistemas que proporcionan dicha información.

• La creciente vulnerabilidad y un amplio espectro de amenazas, tales como las "Cyber amenazas" y la guerra de información

• La escala y el costo de las inversiones actuales y futuras en información y en tecnología de información.

• El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos.

Para muchas organizaciones, la información y la tecnología que la soporta, representan los activos más valiosos de la empresa.

Es más, en nuestro competitivo y rápidamente cambiante ambiente actual, la gerencia ha incrementado sus expectativas relacionadas con la entrega de servicios de IT. Verdaderamente, la información y los sistemas de información son "penetrantes" en las organizaciones (desde la plataforma del usuario hasta las redes locales o amplias, cliente servidor y equipos *Mainframe*. Por lo tanto, la administración requiere niveles de servicio que presenten incrementos en calidad, en funcionalidad y en facilidad de uso, así como un mejoramiento continuo y una disminución de los tiempos de entrega) al tiempo que demanda que esto se realice a un costo más bajo. ***Muchas organizaciones reconocen los beneficios potenciales que la tecnología puede proporcionar. Las organizaciones exitosas, sin embargo, también comprenden y administran los riesgos asociados con la implementación de nueva tecnología.*** Por lo tanto, la administración debe tener una apreciación por, y un entendimiento básico de los riesgos y limitantes del empleo de la tecnología de información para proporcionar una dirección efectiva y controles adecuados. COBIT ayuda a salvar las brechas existentes entre riesgos de negocio, necesidades de control y aspectos técnicos. Proporciona "prácticas sanas" a través de un Marco Referencial de dominios y procesos y presenta actividades en una estructura manejable y lógica. Las **prácticas sanas** de COBIT representan el consenso de los expertos (le ayudarán a optimizar la inversión en información, pero aún más importante, representan aquello sobre lo que usted será juzgado si las cosas salen mal.

Las organizaciones deben cumplir con requerimientos de calidad, de reportes fiduciarios y de seguridad, tanto para su información, como para sus activos. La administración deberá obtener un balance adecuado en el empleo de sus recursos disponibles, los cuales incluyen: personal, instalaciones, tecnología, sistemas de aplicación y datos. Para cumplir con esta responsabilidad, así como para alcanzar sus expectativas, la administración deberá establecer un sistema adecuado de control interno. Por lo tanto, este sistema o marco referencial deberá

existir para proporcionar soporte a los procesos de negocio y debe ser preciso en la forma en la que cada actividad individual de control satisface los requerimientos de información y puede impactar a los recursos de IT. El impacto en los recursos de IT es enfatizado en el Marco Referencial de COBIT conjuntamente a los requerimientos de información del negocio que deben ser alcanzados: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. El control, que incluye políticas, estructuras, prácticas y procedimientos organizacionales, es responsabilidad de la administración.

Un Objetivo de Control en IT es una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control específicos dentro de una actividad de IT.

La orientación a negocios es el tema principal de COBIT. Este diseñado no solo para ser utilizado por usuarios y auditores, sino que en forma más importante, está diseñado para ser utilizado como una lista de verificación 8 detallada para los propietarios de los procesos de negocio.

COBIT es una herramienta que permite a los gerentes comunicarse y salvar la brecha existente entre los requerimientos de control, aspectos técnicos y riesgos de negocio. COBIT habilita el desarrollo de una política clara y de buenas prácticas de control de IT a través de organizaciones, en el ámbito mundial. El objetivo de COBIT es proporcionar estos objetivos de control, dentro del marco referencial definido, y obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo.

Por lo tanto, COBIT está orientado a ser la herramienta de gobierno de IT que ayude al entendimiento y a la administración de riesgos asociados con tecnología de información y con tecnologías relacionadas**.**

4.2.9 Marco Referencial

El Marco Referencial de COBIT proporciona herramientas al propietario de procesos de negocio que facilitan el cumplimiento de esta responsabilidad. El Marco Referencial comienza con una premisa simple y práctica:

Con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos, los recursos de IT deben ser administrados por un conjunto de procesos de IT agrupados en forma natural.

Continúa con un conjunto de 34 Objetivos de Control de alto nivel, uno para cada uno de los Procesos de IT, agrupados en cuatro dominios: planeación y organización, adquisición e implementación, entrega (de servicio) y monitoreo. Esta estructura cubre todos los aspectos de información y de la tecnología que la soporta. Dirigiendo estos 34 Objetivos de Control de alto nivel, el propietario de procesos de negocio podrá asegurar que se proporciona un sistema de control adecuado para el ambiente de tecnología de información. Adicionalmente, correspondiendo a cada uno de los 34 objetivos de control de alto nivel, existe una guía de auditoría o de aseguramiento que permite la revisión de los procesos de IT contra los 34 objetivos detallados de control recomendados por COBIT para proporcionar a la Gerencia la certeza de su cumplimiento y/o una recomendación para su mejora.

El Marco Referencial COBIT otorga especial importancia al impacto sobre los recursos de IT, así como a los requerimientos de negocios en cuanto a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad que deben ser satisfechos. Además, el Marco Referencial proporciona definiciones para los requerimientos de negocio que son derivados de objetivos de control superiores en lo referente a calidad, seguridad y reportes fiduciarios en tanto se relacionen con Tecnología de Información.

La administración de una empresa requiere de prácticas generalmente aplicables y aceptadas de control y gobierno en IT para medir en forma comparativa tanto su ambiente de IT existente, como su ambiente planeado.

El desarrollo de este Marco Referencial de objetivos de control para IT, conjuntamente con una investigación continua aplicada a controles de IT constituye el fundamento para el progreso efectivo en el campo de los controles de sistemas de información.

4.2.10 Audiencia: Administración, Usuarios y Auditores.

COBIT está diseñado para ser utilizado por tres audiencias distintas:

Administración: Para ayudarlos a lograr un balance entre los riesgos y las inversiones en control en un ambiente de tecnología de información frecuentemente impredecible.

Usuarios: Para obtener una garantía en cuanto a la seguridad y controles de los servicios de tecnología de información proporcionados internamente o por terceras partes.

Auditores de sistemas de información: Para brindar soporte a las opiniones mostradas a la administración sobre los controles internos.

Además de responder a las necesidades de la audiencia inmediata de la Alta Gerencia, a los auditores y a los profesionales dedicados al control y seguridad, *COBIT* puede ser utilizado dentro de las empresas por el propietario de procesos de negocio en su responsabilidad de control sobre los aspectos de información del proceso, y por todos aquéllos responsables de IT en la empresa.

En resumen de los 34 procesos que COBIT, se detallan de la siguiente manera:

- **Planear y organizar.**

PO1 Definir un Plan Estratégico de Tecnología de Información

PO2 Definir la Arquitectura de Información

PO3 Determinar la dirección tecnológica

PO4 Definir los procesos de TI, su Organización y las Relaciones de TI

PO5 Manejar la Inversión en TI

PO6 Comunicar la dirección y aspiraciones de la gerencia

PO7 Administrar Recursos Humanos

PO8 Administrar con Calidad

PO9 Evaluar y administrar los Riesgos

PO10 Administrar proyectos

- **Adquirir e Implementar**

DS1 Definir y administrar Niveles de Servicio

DS2 Administrar Servicios prestados por Terceros

DS3 Administrar Desempeño y Capacidad

DS4 Asegurar un Servicio Continuo

DS5 Garantizar la Seguridad de Sistemas

DS6 Identificar y Asignar Costos

DS7 Educar y Entrenar a Usuarios

- **Entregar y Soportar**

DS8 Administrar la Mesa de Servicio y los Incidentes

DS9 Administrar la Configuración

DS10 Administrar Problemas

DS11 Administrar Datos

DS12 Administrar el ambiente físico

DS13 Administrar Operaciones

- **Monitorear y Evaluar**

ME1 Monitorear y Evaluar el desempeño de TI

ME2 Monitorear y Evaluar el Control Interno

ME3 Asegurar el cumplimiento con Requerimientos externos

4.2.11 Usuarios de Interés del modelo COBIT:

- La Gerencia: para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.
- Los Usuarios Finales: quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.
- Los Auditores: para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.
- Los Responsables de TI: para identificar los controles que requieren en sus áreas. También puede ser utilizado dentro de las empresas por el responsable de un proceso de negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de la TI en las empresas.

4.2.12 Características del COBIT.

- Orientado al negocio
- Alineado con estándares y regulaciones "de facto"
- Basado en una revisión crítica y analítica de las tareas y actividades en TI • Alineado con estándares de control y auditoria (COSO, IFAC, IIA, ISACA, AICPA).

4.2.13 Principios del COBIT.

El enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con las TI que deben ser administrados por procesos de TI. Requerimientos de la información del negocio: Para alcanzar los requerimientos de negocio, la información necesita satisfacer ciertos criterios:

Requerimientos de Calidad: Calidad, Costo y Entrega. Requerimientos Fiduciarios: Efectividad y Eficiencia operacional, Confiabilidad de los reportes financieros y Cumplimiento le leyes y regulaciones.

Requerimientos de seguridad: confidencialidad, integridad y disponibilidad.

- **Eficiencia**: Se debe proveer información mediante el empleo óptimo de los recursos (la forma más productiva y económica).
- **Confiabilidad:** Proveer la información apropiada para que la administración tome las decisiones adecuadas para manejar la empresa y cumplir con sus responsabilidades.
- **Cumplimiento:** De las leyes, regulaciones y compromisos contractuales con los cuales está comprometida la empresa.
- **Confidencialidad:** Protección de la información sensible contra divulgación no autorizada.
- **Integridad:** Refiere a lo exacto y completo de la información así como a su validez de acuerdo con las expectativas de la empresa.
- **Disponibilidad:** Accesibilidad a la información cuando sea requerida por los procesos del negocio y la salvaguarda de los recursos y capacidades asociadas a la misma.

4.2.14 Recursos en Tecnología de la información.

En COBIT se establecen los siguientes recursos en TI necesarios para alcanzar los objetivos de negocio:

1. **Datos:** Todos los objetos de información. Considera información interna y externa, estructurada o no, gráficas, sonidos, etc.
2. **Aplicaciones:** Entendidas como sistemas de información, que integran procedimientos manuales y sistematizados.

3. **Tecnología:** incluye hardware y software básico, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, etc.

4. **Instalaciones:** Incluye los recursos necesarios para alojar y dar soporte a los sistemas de información.

5. **Recurso humano:** Por la habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorear los sistemas de Información, o de procesos de TI.

4.3 EMPRESA: COMISARIATO DE LA POLICIA NACIONAL.

4.3.1 Visión:

Ser la primera opción de compra de los miembros de Gobernación, garantizándoles ahorro y satisfacción con atención personalizada y excelente servicio.

4.3.2 Misión:

Satisfacer las necesidades de nuestros clientes en el consumo de productos alimenticios, electrodomésticos, ropa, calzado; a los precios más bajos del mercado, ofreciendo un excelente abastecimiento y surtido en las líneas de productos.

4.3.3 Valores.

Los valores que la empresa desarrolla en su entorno laboral para mejorar su calidad de entorno son:

- Integridad.
- Honestidad
- Responsabilidad.
- Respeto.
- Eficiencia.
- Creatividad.
- Trabajo en equipo.

4.3.4 Antecedentes del Comisarito de la Policía Nacional de Masaya.

El comisariato de la policía Nacional fue fundado en Managua en 01 de mayo del año 1999, como respuestas a las necesidades del Sector del Ministerio de Gobernación, brindándoles un servicio que les garantice recursos para sus hogares, implementando un método de crédito descontados de sus salarios y sin ningún interés adicional, beneficiando a gran parte este sector nicaragüense. Fue creado con fondos de la Policía Nacional en base a la Ley No. 228 de la Policía Nacional y con fondos provenientes de la Rifa de dos vehículos donados por Amigos de la Policía Nacional.

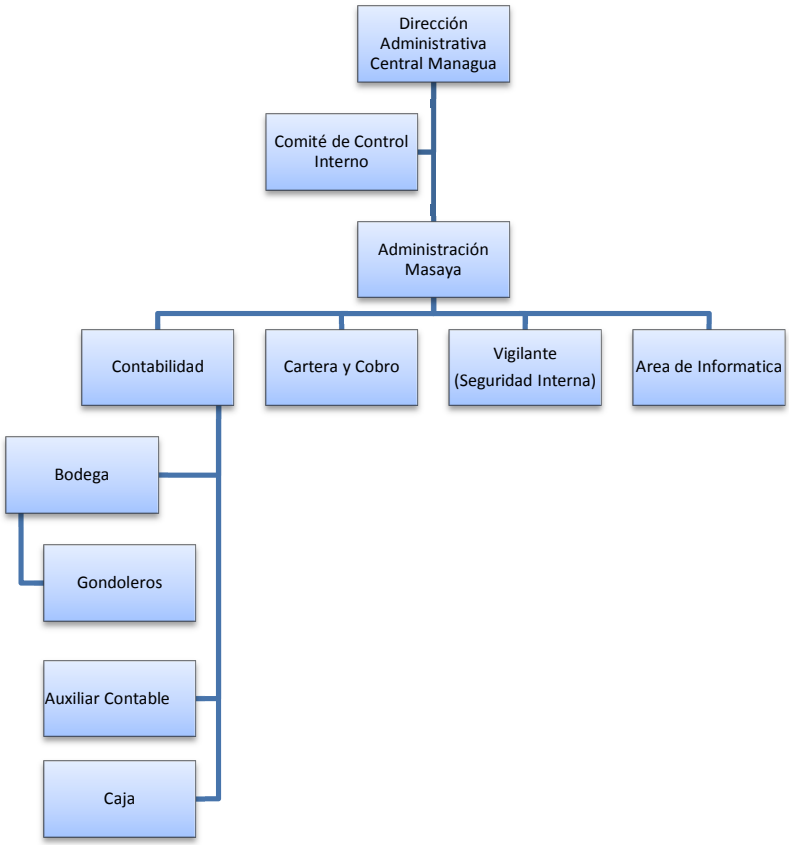
El comisariato de la Policial Nacional en busca de suplir con las necesidades de más hogares abrió otras sucursales en los departamentos de: Masaya, Chinandega, León y Bluefields.

El comisariato de la policía Nacional de la sucursal Masaya, se inauguró el 20 de julio del 2010. Brindando la venta de productos abarrotería, cuidado personal y productos del hogar. Atendiendo a todo el área sur-oriente (Los pueblos blancos, Granada, Nandaime, Jinotepe, etc.).

Como nueva política, la administración de este comisariato ha resuelto atender a personas naturales que no pertenecen a la institución del Ministerio de Gobernación, pero realizando ventas de contado. También ha creado acuerdos con otras instituciones como diversas alcaldías del Municipio de Masaya, ENACAL, etc. Todo esto para ampliar su mercado y competir con otros negocios de esta índole.

4.3.5 Organigrama de la empresa.

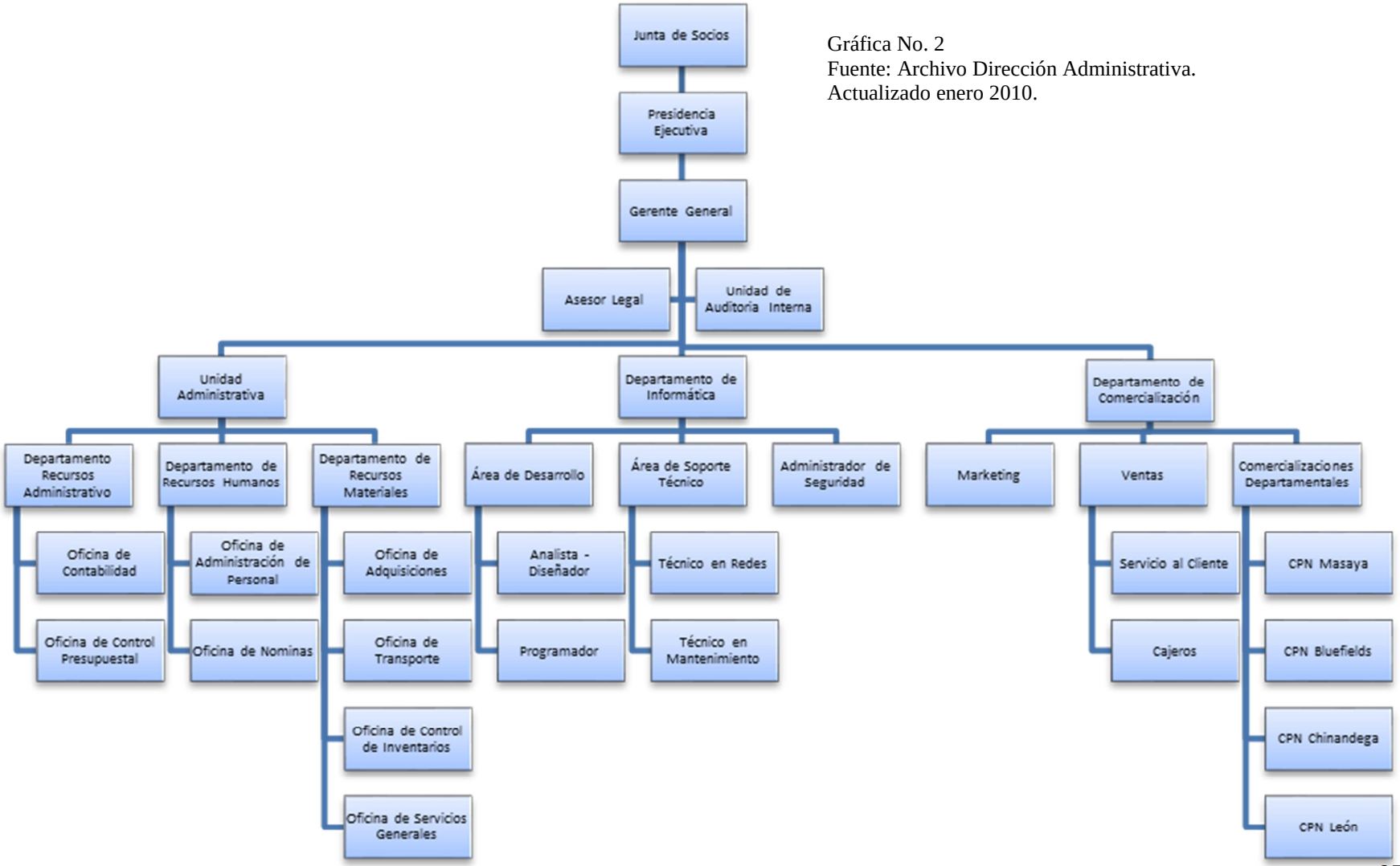
La estructura orgánica del Comisariato de la Policía Nacional Masaya está dada de la siguiente manera:



Gráfica No. 1
Fuente: Archivo Dirección Administrativa Masaya.
Actualizado mayo 2011.

4.3.6 Organigrama del Comisariato de la Policía Nacional Managua.

Quien es el que regula las Actividades y las dependencia Departamentales.



Gráfica No. 2
Fuente: Archivo Dirección Administrativa.
Actualizado enero 2010.

4.3.6 Generalidades del Sistema SGA (Sistema de Gestión Administrativa)

La empresa usa el sistema SGA (Sistema de Gestión Administrativa), el cual además comprende soluciones para Ventas, Compras, Almacén, Activos y Remuneraciones, todos integrados con el sistema de contabilidad mediante los asientos contables por cada área.

El SGA es un sistema eficiente, fácil de usar, funcional y efectivo para agilizar las ventas, sistematizar el trabajo y obtener toda la información de gastos, ganancias y ventas. (Windows 8).

El módulo de Gestión reside en un servidor y permite el mantenimiento de los artículos, precios, stock, proveedores, clientes, cheques, etc. Comunica esta información a las cajas (POS) mediante una red local.

Algunas de las características del programa son las siguientes:

• Permite la facturación de artículos mediante cualquier lector de códigos de barra o por teclado. (El código de barras puede ser igual o distinto al código interno. El código interno puede ser el código que usa el proveedor cuando factura el artículo, de esta forma el ingreso de compras se agiliza.)

• Permite facturar ventas por departamentos y por peso (Para artículos que se vende con una etiqueta de códigos de barra impresa por la balanza.)

• Compatible con controladores fiscales homologados Hasar, NCR y Epson.

• Envases

• Gestión de precios con actualización automática de precio de costo y ventas por familia y/o proveedor.

• Control de stock con simple gestión administrativa.

• Puede emitir tickets a consumidor final y ticket-factura “A” para responsables inscriptos.

• Reportes estadísticos de : Ventas por articulo y familia. Clientes ranking y detallado por artículos. Proveedores por compras y mercaderías. Cuentas corrientes: Clientes y cobranzas. Proveedores y pagos. Costos y ganancia

Este sistema permite administrar, a través de un modulo de gestión administrativa (1), el control de stock e inventario, actualización de precios, emisión de etiquetas, cuentas corrientes de clientes y proveedores, reportes estadísticos de ventas, control de balanzas digitales, compras y gastos, caja y bancos, etc.

Sistema de Gestión (Back Office / Administración)

El módulo de Gestión reside en un servidor y permite el mantenimiento de los artículos, precios, stock, proveedores, clientes, cheques, etc. Comunica esta información a las cajas (POS) mediante una red local y recolecta las ventas de las mismas actualizando las estadísticas y el stock. Por otro lado, permite llevar las cuentas corrientes con los clientes y proveedores, emitir órdenes de pago, analizar vencimientos, confeccionar el libro de IVA compras, imprimir etiquetas con los precios para las góndolas, carteles con ofertas, listados de stock, listados de reposición, valorización del inventario, etc.

Punto de Venta (POS)

El módulo de Punto de Venta (POS) reside en PC's individuales conectadas en red con el servidor. Permite emitir ticket y ticket-factura A y B por medio de un controlador fiscal.

Aunque todas las cajas estén en red, mientras están facturando no es necesario que la red esté activa. Es decir, el POS puede funcionar como independientemente ya que cada una posee autonomía. De esta forma si se cae la red los puestos de venta siguen funcionando. La red sirve para transmitir los datos hacia y desde las cajas al servidor. O sea, se efectúa la recolección de ventas de cada caja y, a su vez, el programa de gestión le envía a esa caja el archivo maestro de artículos con los nuevos precios.

Quiere decir que el sistema de gestión actualiza los POS, recibiendo de ellos la información de ventas y enviándole los nuevos precios.

4.3.7 Unidad de Auditoria del Comisariato de la Policía Nacional.

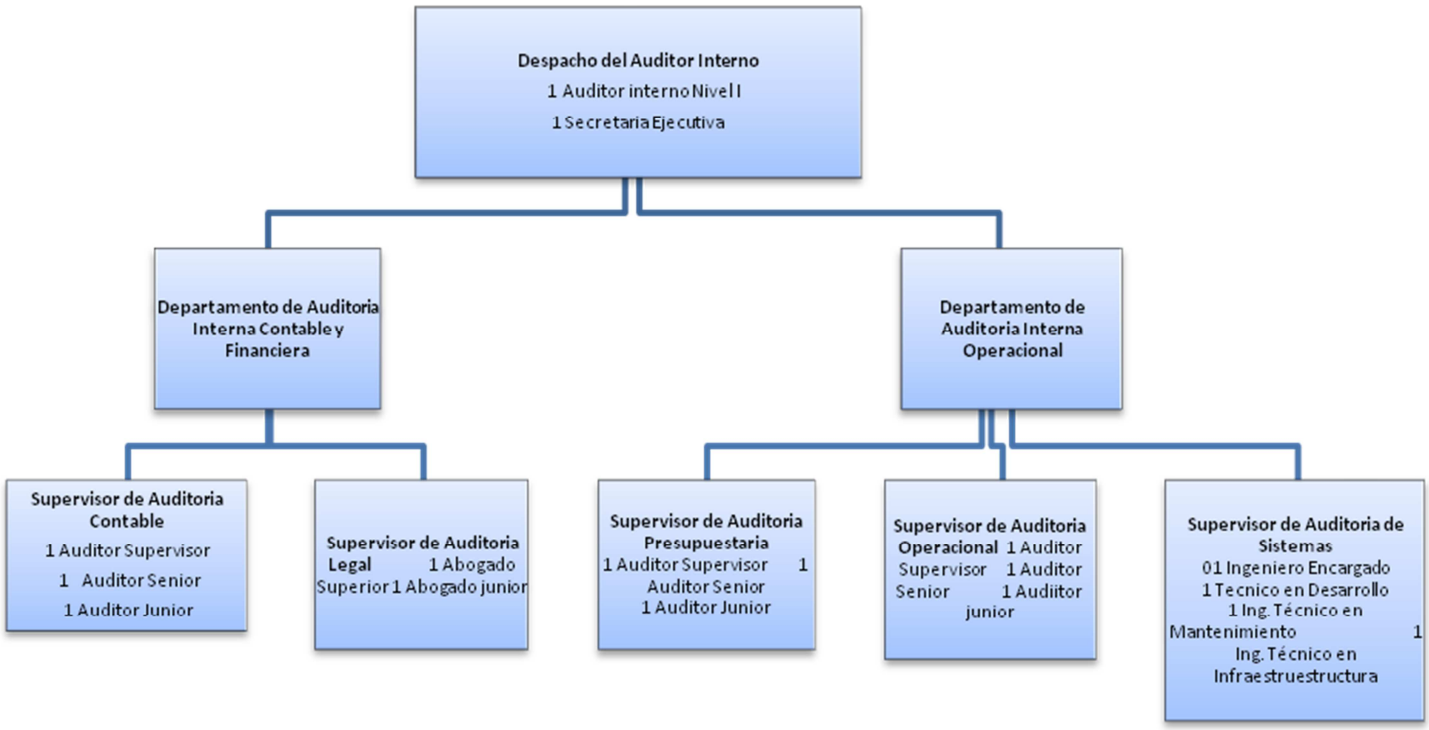
La gestión moderna exige una constante búsqueda y aplicación de técnicas idóneas que permitan la sistematización y homogeneidad de los procesos, de manera que se conjuguen la eficiencia y la eficacia. Exigencia de la que no se escapa el Comisariato de la Policía Nacional por ser un ente de naturaleza privada, estando sustentado su adecuado funcionamiento al fiel cumplimiento de las leyes, reglamentos y normas que regulan los procesos de la Administración, aplicando al desarrollo organizacional estratégico, objetivos, funciones y estructura organizativa de la Unidad de Auditoría Interna, con el propósito de facilitar el logro del objetivo trazado.

Objetivos organizacionales:

La Unidad de de Auditoría Interna del Comisariato de la Policía Nacional tiene como objetivo, evaluar el sistema de control interno, incluyendo el grado de operatividad y eficacia de los sistemas de administración y de información gerencial, así como el examen de los registros y estados financieros, para determinar su pertinencia y confiabilidad.

La evaluación de la eficiencia, eficacia y economía en el marco de las operaciones realizadas, igualmente la Unidad de Auditoría Interna en el ámbito de su competencia, podrá realizar auditorías, inspecciones, fiscalizaciones, exámenes, estudios, análisis e investigaciones de todo tipo y de cualquier naturaleza para verificar la legalidad, exactitud, sinceridad y corrección de sus operaciones, así como para evaluar el cumplimiento y los resultados de los planes y las acciones administrativas, la eficacia, eficiencia, economía, calidad e impacto de las mismas.

La unidad de Auditoria del Comisariato de la Policía Nacional está estructurada orgánicamente de la siguiente manera:



Grafica No. 3
Fuente: Archivo del Despacho del Auditor Interno.
Actualizado enero 2010.

4.4 Auditoría Interna de tecnología de la Información.

4.4.1. Origen de la auditoria:

La presente auditoria se realiza en cumplimiento del plan anual de control 2014, aprobada mediante la resolución n° 201del 15 de diciembre del 2013.

4.4.2 Objetivos y alcance de la auditoria

4.4.3.1 Objetivo general.

- ✓ Revisar y evaluar los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

4.4.3.2 Objetivos específicos.

- ✓ Evaluar el diseño y prueba de los sistemas del área de informática
- ✓ Determinar la veracidad de la información del área de informática
- ✓ Evaluar los procedimientos de control de operación, analizar su estandarización y evaluar el cumplimiento de los mismos.
- ✓ Evaluar la forma como se administran los dispositivos de almacenamiento básico del área de informática.

4.4.4 Enfoque a utilizar.

- La presente acción de control, se realiza de acuerdo al COBIT 4, que se enfocan en la administración y control de la tecnología de información dentro de la organización, sirviendo como un marco de referencia que clasifica los procesos de las unidades de tecnología de información. Y También de acuerdo a las Normas para el Ejercicio Profesional de la Auditoría Interna (NIEPAI), habiéndose aplicado procedimientos de Auditoria que se consideraron necesarios de acuerdo a las circunstancias.
- La presente Auditoria Informática se realizara en el Comisariato de la Policía Nacional, ubicado en la localidad de Masaya, siendo el área a examinarse la de Informática.

4.4.5 Relación de asignación de equipos informáticos y cargos del área a examinar.

La empresa cuenta con 6 equipos de cómputos distribuidos de la siguiente manera: * Todo el software se encuentra debidamente licenciado.

Equipo	Localización	Asignado a:	Usuario	Características del Software	Características del Hardware
CPU Optiplex 755	Administración /Servidor	Antonio Cruz	ACRUZ	Una plataforma de sistema operativo de Windows XP y Windows 7 , trabajando con funcionalidad multiusuario, desarrollado en el lenguaje de Microsoft Visual Studio 2010 y como sistema gestor de base de datos SQL Server 2008.	Procesador 2.3 Ghz Memoria RAM: 4 Gb Sistema operativo: Windows Server 2008. Espacio total en disco duro: 1 TB Número de usuarios: 15
CPU Optiplex 755	Administración	Antonio Cruz	ACRUZ	Microsoft Office 2010, Adobe Acrobat ,WinZip, Antivirus Kaperski, Correo electrónico Outlook Sistema Gestion Administrativa (SGA)	Procesador: 1.8 Ghz Memoria RAM: 2 GB Sistema operativo: Windows XP Espacio total en disco duro: 500 Gb Número de usuarios: 1
CPUOptiplex 160L	Facturación	María Mendoza	MMENDOZA	Microsoft Office 2010 Adobe Acrobat WinZip Antivirus Kaperski Correo electrónico Outlook Sistema Gestion Administrativa (SGA)	Procesador: 1.8 Ghz Memoria RAM: 2 GB Sistema operativo: Windows XP Espacio total en disco duro: 500 Gb Número de usuarios: 1
CPU Dell GX 520	Facturación	Teresa Urbina	TURBINA	Microsoft Office 2010 Adobe Acrobat WinZip Antivirus Kaperski Correo electrónico Outlook Sistema Gestion Administrativa (SGA)	Procesador: 1.8 Ghz Memoria RAM: 2 GB Sistema operativo: Windows XP Espacio total en disco duro: 500 Gb Número de usuarios: 1
CPU Dell GX 520	Bodega	Ronny Ortega	RORTEGA	Microsoft Office 2010 Adobe Acrobat WinZip Antivirus Kaperski Correo electrónico Outlook Sistema Gestion Administrativa (SGA)	Procesador: 1.8 Ghz Memoria RAM: 2 GB Sistema operativo: Windows XP Espacio total en disco duro: 500 Gb Número de usuarios: 1
CPU Dell Optiplex 520	Contabilidad	Lauren Ruiz	LRUIZ	Microsoft Office 2010 Adobe Acrobat WinZip Antivirus Kaperski Correo electrónico Outlook Sistema Gestion Administrativa (SGA)	Procesador: 1.8 Ghz Memoria RAM: 2 GB Sistema operativo: Windows XP Espacio total en disco duro: 500 Gb Número de usuarios: 1
CPU Dell Optiplex	Cartera y Cobro	Lester Cuadra	LCUADRA	Microsoft Office 2010 Adobe Acrobat WinZip Antivirus Kaperski Correo electrónico Outlook Sistema Gestion Administrativa (SGA)	Procesador: 1.8 Ghz Memoria RAM: 2 GB Sistema operativo: Windows XP Espacio total en disco duro: 500 Gb Número de usuarios: 1

4.4.6 Cronograma de trabajo

PROGRAMA DE AUDITORIA			
Empresa: CPN Masaya		**Fecha: 15/01/2014**	**Hoja No. 01**
Fase	**Actividad**	**Horas Estimadas**	**Encargados**
I	VISITA PRELIMINAR: • Solicitud de Manuales y Documentaciones. • Elaboración de los cuestionarios. • Recopilación de la información organizacional: estructura orgánica, recursos humanos, presupuestos.	**3500**	**Auditor Encargado Supervisores**
II	DESARROLLO DE LA AUDITORIA • Aplicación del cuestionario al personal. • Entrevistas a líderes y usuarios más relevantes de la dirección. • Análisis de las claves de acceso, control, seguridad, confiabilidad y respaldos. • Evaluación de la estructura orgánica: departamentos, puestos, funciones, autoridad y responsabilidades. • Evaluación de los Recursos Humanos y de la situación Presupuestal y Financiera: desempeño, capacitación, condiciones de trabajo, recursos en materiales y financieros mobiliario y equipos. • Evaluación de los sistemas: relevamiento de • Hardware y Software, evaluación del diseño lógico y del desarrollo del sistema. • Evaluación del Proceso de Datos y de los • Equipos de Cómputos: seguridad de los datos, control de operación, seguridad física y procedimientos de respaldo.	**8950**	
III	REVISION Y PRE-INFORME • Revisión de los papeles de trabajo. • Determinación del Diagnostico e Implicancias. • Elaboración de la Carta de Gerencia. • Elaboración del Borrador.	**2070**	
IV	INFORME • Elaboración y presentación del Informe.	**200**	

4.4.7 Documentos a solicitar para realizar la auditoria.

- Políticas, estándares, normas y procedimientos.
- Plan de sistemas.
- Planes de seguridad y continuidad
- Contratos, pólizas de seguros.
- Organigrama y manual de funciones.
- Manuales de sistemas.
- Registros
- Entrevistas
- Archivos
- Requerimientos de Usuarios.

4.8.1 Área informática

- **Misión:**

El área de informática del comisariato de la policía nacional tiene por misión normar el adecuado uso y aprovechamiento de los recursos informáticos; la optimización de las actividades, servicios procesos y acceso inmediato a información para la toma de decisiones, mediante el desarrollo, implantación y supervisión del correcto funcionamiento de los sistemas.

- **Visión:**

El área de informática, del CPN Masaya es ser capaz de liderar el desarrollo informático, asegurando un marco transparente para el acceso a los usuarios a la información.

- **Situación actual.**

Ubicación: El área de informática orgánicamente depende de la oficina de Planificación y presupuesto, asumiendo la responsabilidad de dirigir los procesos técnicos de informática.

- **Recursos Humanos:**

Actualmente en el área de cómputo e informática labora una sola persona quien cumple las funciones de administración, capacitación, soporte y procesamiento de datos.

- **Recursos informáticos existentes:**

Servidor CPU Optiplex	1
Computadoras	6

Personales	
Impresoras	2

4.4.8.2 Análisis FODA

Fortalezas

- Disponibilidad de recursos económicos.
- Personal Directivo y técnico con amplia experiencia(recursos humanos)
- Capacidad de Convocatoria (Difusión).

Oportunidades

- Búsqueda de reducción de costos, aprovechando la aparición de nuevas tecnologías.
- Buen servicio y trato.
- Tendencias Tecnológicas generan un amplio campo de acción.
- Predisposición y voluntad de los nuevos directivos para cambio Tecnológico.

Debilidades

- Falta de planes y Programas Informáticos.
- Poca identificación del personal con la empresa.
- Inestabilidad laboral del personal.
- Escasa capacidad de retención y voluntad del personal.
- No existe programas de capacitación y actualización al personal.
- La oficina de informática es muy reducida.
- Personal técnico Calificado insuficiente en el área informática.

Amenazas

- Rotación permanente del personal imposibilitando continuidad a los objetivos propuestos.

4.4.8.3 Justificación de la auditoría.

- Aumento considerable e injustificado del presupuesto del PAD (Departamento de Procesamiento de Datos)
- Desconocimiento en el nivel directivo de la situación informática de la empresa

- Falta total o parcial de seguridades lógicas y físicas que garanticen la integridad del personal, equipos e información.
- Falta de una planificación informática.
- Organización que no funciona correctamente, falta de políticas, objetivos, normas, metodología, asignación de tareas y adecuada administración del Recurso Humano.
- Descontento general de los usuarios por incumplimiento de plazos y mala calidad de los resultados.

4.4.8.4 Motivo o necesidad de una auditoria informática.

1. **Síntomas de descoordinación y desorganización:**

- No coinciden los objetivos del área de Informática y de la propia empresa.
- Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente. Puede ocurrir con algún cambio masivo de personal, o en una reestructuración fallida de alguna área o en la modificación de alguna norma importante.

2. **Síntomas de mala imagen e insatisfacción de los usuarios:**

- No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de software en los terminales de usuario, refrescamiento de paneles, variación de los ficheros que deben ponerse diariamente a su disposición, etc.
- No se reparan las averías de hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.
- No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de Aplicaciones críticas y sensibles.

3. **Síntomas de debilidades económico-financiero:**

- Incremento desmesurado de costos.
- Necesidad de justificación de Inversiones Informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).
- Costos y plazos de nuevos proyectos (deben auditarse simultáneamente a
- Desarrollo de Proyectos y al órgano que realizó la petición).

V. Caso Práctico.

(Desarrollo de la Auditoría)

La auditoría interna de Tecnología de la información se desarrollada en el Comisariato de la Policía Nacional Masaya, está dada de la siguiente manera:

Primeramente se presentan Horas y Distribución de horas disponibles de la auditoria (pág. 46 y 47), Plan de trabajo (Pág. 48 y 49), Presupuesto de tiempo y Costo de la auditoria.

A continuación se plantean las auditorías realizadas por áreas a inspeccionar, los cuales se realizaron a través de entrevistas al personal del CPN Masaya, con la finalidad de identificar los errores y debilidades en el área informática.

Las auditorias se desarrollaron de la siguiente manera:

Auditoria de Mantenimiento
Auditoria de Base de Datos
Auditoria de Calidad
Auditoria de Seguridad
Auditoria de Sistemas de Redes
Auditoria de Aplicaciones
Auditoria Física
Auditoria de Dirección
Auditoria de Explotación
Auditoria de Desarrollo.
Auditoria de Ofimática

5.1 Estructura organizacional del área de sistema.
(Controles sobre las actividades TI)

Se ejecutarán los siguientes procedimientos:

5.1.1 Estructura del personal

	COBIT		
PROCEDIMIENTOS	DOMINIO	CODIGO	OBJETIVOS DE CONTROL
Dependencia, roles y responsabilidades del personal del área informática.	Planeación Y Organización	PO4	Definición de la Organización y de las Relaciones IT
Evaluación de la segregación de funciones.	Planeación Y Organización	PO4	Definición de la Organización y de las Relaciones IT – Segregación de Funciones
Análisis del perfil de cada cargo tipo y sus ocupantes (experiencia, capacitación y escolaridad).	Planeación Y Organización	PO4	Administración de Recursos Humanos

5.2 Evaluación de Gestión.

	COBIT		
PROCEDIMIENTOS	DOMINIO	CODIGO	OBJETIVO DE CONTROL
Evaluar los procesos y estándares probar su cumplimiento	Planeación y organización	PO4	Comunicación de la dirección y aspiraciones de la gerencia comunicación de Las políticas de la empresa
Evaluar el proceso de planeamiento y la razonabilidad del plan informático respecto a los objetivos de la organización.	Planeación y organización	PO1	Definición de un Plan Estratégico de Tecnología de Información
Evaluar los procedimientos de asignación de recursos y la elaboración y administración de presupuestos, así como la razonabilidad de los recursos asignados.	Planeación y organización	PO10	Administración de proyectos

5.3 Atención al usuario.

	COBIT		
PROCEDIMIENTOS	DOMINIO	CODIGO	OBJETIVO DE CONTROL
Análisis del procedimiento establecido para asegurar que el servicio sea acorde con las necesidades de los usuarios.	Entrega de Servicios y Soporte	DS8	Apoyo y Asistencia a los Clientes de Tecnología de Información.
Evaluación de los procedimientos de atención a usuarios y administración de problemas.	Entrega de Servicios y Soporte	DS8	Administración de problemas e incidentes

5.4 Gestión de los sistemas informáticos.

	COBIT		
PROCEDIMIENTOS	DOMINIO	CODIGO	OBJETIVOS DE CONTROL
Revisar y evaluar la metodología de desarrollo de aplicaciones existente.	Planeación y organización	PO11	Administración de calidad– metodología del ciclo de vida de desarrollo de sistemas
Relevar los procedimientos para desarrollo de aplicaciones utilizados.	Planeación y organización	PO11	Administración de calidad
Evaluar los procedimientos e iniciativas de investigación y desarrollo.	Planeación y organización	PO10	Administración de proyectos
Revisar la documentación de la planificación de mantenimiento / mejora de aplicaciones, así como la documentación que sustenta la prueba y otros procesos de recepción por parte del usuario.	Adquisición e implementación	AI12	Adquisición y mantenimiento del software de aplicación

5.5 Desarrollo, Operación y Mantenimiento de Aplicaciones.

	COBIT		
PROCEDIMIENTOS	DOMINIO	CODIGO	OBJETIVOS DE CONTROL
Evaluar los procedimientos de operación.	Adquisición e Implementación	AI4	Procedimientos relacionados con la Tecnología de la Información
Revisar las bitácoras de operación.	Planeación y organización	AI4	Desarrollo y Mantenimiento de procedimientos relacionados con la Tecnología de la Información
Revisar los procedimientos y revisar las bitácoras de ejecución de los procesos batch.	Entrega de servicios y Soportes	DS13	Administración de Operaciones
Revisar los procedimientos vigentes para backup de información (tipo de información, periodicidad, lugar de almacenamiento y pruebas periódicas de los respaldos).	Entrega de servicios y Soportes	DS11	Administración de la Información

Administración de las Bases de Datos.

	COBIT		
PROCEDIMIENTOS	DOMINIO	CODIGO	OBJETIVOS DE CONTROL
Evaluar los procedimientos de administración de la base de datos.	Planeación y organización	PO2	Definición de la arquitectura de Información.
Revisar el sistema de documentación de la base de datos (nivel de detalle y actualización de la información).	Planeación y organización	PO2	Definición de la arquitectura de información.
Analizar roles y responsabilidades de la administración de la base de datos.	Planeación y organización	PO2	Definición de la arquitectura de información

Gestión y explotación de las Aplicaciones.

	COBIT		
PROCEDIMIENTOS	DOMINIO	CODIGO	OBJETIVOS DE CONTROL
Relevar información relativa a las aplicaciones como: Características generales Responsables Plataforma tecnológica Principales módulos Mecanismos de seguridad disponibles Documentación existente Interfaces con otros sistemas Implantaciones en curso	Adquisición e implementación	AI2	Adquisición y Mantenimiento de software de aplicación
Evaluar la seguridad y control de cada aplicación	Entrega de servicios y Soporte	DS5	Garantizar la Seguridad de Sistemas

Plataformas y Comunicaciones.

	COBIT		
PROCEDIMIENTOS	DOMINIO	CODIGO	OBJETIVO DE CONTROL
Revisión de los procedimientos de medición del rendimiento. Análisis de los informes de rendimiento disponibles.	Entrega de servicios y Soportes	DS3	Administración de desempeño y capacidad
Revisión de los procedimientos relativos al monitoreo de la red. Análisis de la bitácora de problemas.	Entrega de servicios y Soportes	DS3	Administración de desempeño y capacidad.
Análisis de los mecanismos de comunicación y acceso a los datos de la red desde el punto de vista de disponibilidad.	Entrega de servicios y Soportes	DS3	Administración de desempeño y capacidad.
Relevar las herramientas de monitoreo de hardware y software existentes, compararlas con las disponibles en el mercado.	Entrega de servicios y soportes	DS3	Administración de desempeño y capacidad.
Revisar procedimientos de respaldo (líneas de comunicación alternativas).	Entrega de servicios y soporte	DS4	Aseguramiento de servicio continuo
Relevamiento de la arquitectura del sistema, incluyendo: ♦ Servicios de red implementados ♦ Diagrama de la red	Entrega de servicios y soporte	DS9	Administración de la configuración

5.6 Evaluación de Seguridades y Procedimientos de continuidad.

Se ejecutarán los siguientes procedimientos:

Seguridades: físicas, lógicas y de comunicaciones.

	COBIT		
PROCEDIMIENTOS	DOMINIO	CODIGO	OBJETIVO DE CONTROL
Evaluar las políticas y procedimientos de seguridad vigentes.	Entrega de Servicios y Soportes	DS5	Garantizar la Seguridad de los Sistemas.
Revisar la seguridad lógica implantada en los servidores, así como los parámetros de seguridad relativos a las claves de acceso, utilizando la herramienta de software específicas para cada plataforma Esto comprende, entre otros: ✓ Tipo y longitud mínima y máxima de las claves de acceso. ✓ Manejo de claves de acceso históricas. ✓ Encriptación de claves. ✓ Administración de claves de acceso por servicio. ✓ Rotación de claves de acceso (automático o manual) y periodicidad. ✓ Número de intentos fallido antes de ingresar al sistema. ✓ Número de sesiones simultáneas por usuario ✓ Número de perfiles de usuario.	Entrega de Servicios y Soportes	DS5	Garantizar la Seguridad de los Sistemas.
Tiempo permitido de inactividad en el sistema.	Entrega de Servicios y Soportes.	DS5	Garantizar la Seguridad de Sistemas
Evaluar los mecanismos de protección antivirus.	Entrega de Servicios y Soportes.	DS5	Garantizar la seguridad de Sistemas
Evaluar los mecanismos de seguridad física existentes, incluyendo contratos de seguros existentes.	Entrega de Servicios y Soportes.	DS12	Administración de Instalaciones
Evaluar los mecanismos de seguridad física existentes, incluyendo contratos de seguros existentes.	Entrega de Servicios y Soportes.	DS12	Administración de Instalaciones

5.7 AUDITORIA DEL MANTENIMIENTO EN EL AREA DE INFORMATICA.

1. Objetivos de la Auditoria.
Realizar un informe de Auditoría con el objeto de evaluar el mantenimiento correctivo y preventivo del software.

A03 Supervisión de la Integración del Expediente del Auditor

Dependencia: Alta Gerencia				
Área Auditada: Las instalaciones físicas del área de informática				
Tipo de Auditoria: Informática	**Número de Auditoria: 01**			
Fecha de Inicio:	**Fecha de Término:**			
Periodo Auditado: Enero –Diciembre 2014				
Personal Participante: Encargado de Informática				
	PREGUNTAS	SI	NO	N/A
1	Existe un contrato de mantenimiento.		X	
2	¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo?	X		
3	¿Se lleva a cabo tal programa?	X		
4	¿Existen tiempos de respuesta y de compostura estipulados en los contratos?	X		
5	¿Existe plan de mantenimiento preventivo. ?		X	
6	¿Se notifican las fallas?	X		
7	¿Se les da seguimiento?		X	
8	¿Tiene un plan logístico para dar soporte al producto software?		X	
9	¿Se realizan varios tipos de medidas para poder estimar la calidad del software?		X	
10	¿La mantenibilidad se tiene en cuenta antes de empezar a desarrollar?		X	
11	¿El desarrollador prepara un Plan de Mantenibilidad que establece prácticas específicas de mantenibilidad, así como recursos y secuencias relevantes de actividades?	X		
12	¿Durante el análisis de requerimientos, los siguientes aspectos que afectan a la mantenibilidad, son tomados en cuenta? • Exactitud y organización lógica de los datos. • Los Interfaces (de máquina y de usuario). • Requerimientos de rendimiento. • Requerimientos impuestos por el entorno (presupuesto). Granularidad (detalle) de los requerimientos y su impacto sobre la trazabilidad. • Énfasis del Plan de Aseguramiento de Calidad del Software (SQAP) en el cumplimiento de las normas de documentación	X		

Entrevista 1-2

	PREGUNTAS	SI	NO	N/A
14	¿La responsabilidad del mantenimiento se transfiere a una organización distinta, se elabora un Plan de Transición?		X	
15	¿El mantenedor a menudo se encuentra con un producto software con documentación?	X		
16	¿Si no hay documentación, el mantenedor deberá crearla? ¿Realiza lo siguiente? a. Comprender el dominio del problema y operar con el producto software. b. Aprender la estructura y organización del producto software. c. Determinar qué hace el producto software. Revisar las especificaciones (si las hubiera)	X		
17	¿Documentos como especificaciones, manuales de mantenimiento para programadores, manuales de usuario o guías de instalación pueden ser modificados o creados, si fuese necesario?	X		
18	¿El Plan de Mantenimiento es preparado por el mantenedor durante el desarrollo del software?	X		
19	¿Los elementos software reflejan la documentación de diseño?	X		
20	¿Los productos software fueron suficientemente probados y sus especificaciones cumplidas?	X		
21	¿Los informes de pruebas son correctos y las discrepancias entre resultados actuales y esperados han sido resueltas?	X		
22	¿La documentación de usuario cumple los estándares especificados?	X		
23	¿Los costes y calendarios se ajustan a los planes establecidos?	X		

Entrevista 2-2

Elaboro: _____ Vo. Bo. Del Responsable: _____
Nombre y Firma Nombre y Firma

Auditoria Mantenimiento:
Para hallar el SI
23 - 100%
15 - X
X = 65.21 %

Para hallar el NO
23 - 100%
8 - X
X = 34.78 %

5.7.1 INFORME DE AUDITORIA DE MANTENIMIENTO

1. Identificación del informe

Auditoria del Mantenimiento en el área de informática.

2. Identificación de la Entidad Auditada

Comisariato de la Policía Masaya.

3. Objetivos

- Revisar los contratos y las cláusulas que estén perfectamente definidas en las cuales se elimine toda la subjetividad y con penalización en caso de incumplimiento, para evitar contratos que sean parciales.
- Verificar el cumplimiento del contrato sobre el control de fallas, frecuencia, y el tiempo de reparación.
- Diagnóstico del sistema actual de mantenimiento.
- Verificar el montaje de métodos de recopilación de información en áreas específicas.
- Verificar la existencia de de planes estratégicos de desarrollo.
- Verificación de la efectividad del mantenimiento actual y los desarrollos y programas proyectados.
- Verificar la optimización de almacenes y repuestos.

5. Hallazgos Potenciales

- Pérdida de control
- Pérdida de una fuente de aprendizaje, porque una actividad interna pasa a ser externa.
- Dependencias del suministrador.
- Variaciones en la calidad del producto entregado al usuario final.
- Problemas entre el personal.
- Uso de metodologías para nuevos desarrollos, pero ausencia de ellas para el mantenimiento.
- Tendencia a la desestructuración
- Dificultad progresiva de modificación

- Falta de presupuesto
- Falta de personal
- Falta de apoyo de la Dirección

6. Alcance de la auditoria

Nuestra auditoria, comprende el presente periodo 2014 y se ha realizado especialmente al área de Informática de acuerdo a las normas y demás disposiciones aplicable al efecto.

7. Conclusiones:

- Como resultado de la Auditoria del Mantenimiento en el área de informática realizada al Comisariato Policía Nacional en Masaya, por el período comprendido entre el 02 de Enero al 31 de Diciembre del 2014, podemos manifestar que hemos cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoría.
- El área de Informática presenta deficiencias sobre todo en el debido cumplimiento de sus funciones y por la falta de ellos.

8. Recomendaciones

- Categorizar los tipos de mantenimiento del software y para cada tipo planificar las actividades y tareas a realizar.
- Elaborar un procedimiento organizado para realizar la migración de un producto software desde un entorno operativo antiguo a otro nuevo.
- Establecer un acuerdo o contrato de mantenimiento entre el mantenedor y el cliente y las obligaciones de cada uno estos.
- Elaborar un plan de mantenimiento que incluya el alcance del mantenimiento, quién lo realizará, una estimación de los costes y un análisis de los recursos necesarios.

8. Fecha Del Informe

	PLANEAMIENTO	EJECUCIÓN	INFORME
FECHA			

9. Identificación Y Firma Del Auditor

APELLIDOS Y NOMBRES	CARGO

5.8 AUDITORIA DE BASE DE DATOS

1. Alcance de la auditoria:

Esta auditoría comprende solamente al área de informática del Comisariato Policía Nacional de Masaya, con respecto al cumplimiento del proceso "De Gestión administración de la Base de Datos " de la de manera que abarca la explotación, mantenimiento, diseño carga, post implementación, Los sistemas de gestión de base de datos (SGBD), software de auditoría, sistema operativo protocolos y sistemas distribuidos.

2. Objetivos

- ✓ Verificar la responsabilidad para la planificación de planillas y control de los activos de datos de la organización" (administrador de datos)

- ✓ Verificar la responsabilidad de la administración del entorno de la base de datos" (administrador de la base de datos)
- ✓ Proporcionar servicios de apoyo en aspectos de organización y métodos, mediante la definición, implantación y actualización de Base de Datos y/o procedimientos administrativos con la finalidad de contribuir a la eficiencia.

A03 Supervisión de la Integración del Expediente del Auditor

Dependencia: Alta gerencia				
Área Auditada: Base de datos				
Tipo de Auditoria: Informática	**Número de Auditoria:**			
Fecha de Inicio: 02 de enero 2013	**Fecha de Término:** 31de enero 2014			
Periodo Auditado:				
Personal Participante:				
	PREGUNTAS	**SI**	**NO**	**N/A**
1	Existe equipos o software de SGBD	X		
2	La organización tiene un sistema de gestión de base de datos (SGBD)	X		
3	Los datos son cargados correctamente en la interfaz grafica	X		
4	Se verificará que los controles y relaciones de datos se realizan de acuerdo a Normalización libre de error	X		
5	Existe personal restringido que tenga acceso a la BD	X		
6	El SGBD es dependiente de los servicios que ofrece el Sistema Operativo		X	
7	La interfaz que existe entre el SGBD y el SO es el Adecuado	X		
8	¿Existen procedimientos formales para la operación del SGBD?	X		
9	¿Están actualizados los procedimientos de SGBD?	X		
10	¿La periodicidad de la actualización de los procedimientos es Anual?	X		
11	¿Son suficientemente claras las operaciones que realiza la BD?	X		

Entrevista 1-2

	PREGUNTAS	SI	NO	N/A
13	¿Se procesa las operaciones dentro del departamento de informática?	X		
14	¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos?	X		
15	¿Existe un control estricto de las copias de estos archivos?	X		
16	¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos?	X		
17	¿Se registran como parte del inventario las nuevas cintas magnéticas que recibe el centro de informática?	X		
18	¿Se tiene un responsable del SGBD?	X		
19	¿Se realizan auditorias periódicas a los medios de almacenamiento?		X	
20	¿Se tiene relación del personal autorizado para manipular la BD?		X	
21	¿Se lleva control sobre los archivos trasmitidos por el sistema?		X	
22	¿Existe un programa de mantenimiento preventivo para el dispositivo del SGBD?			X
23	¿Existen integridad de los componentes y de seguridad de datos?	X		
24	De acuerdo con los tiempos de utilización de cada dispositivo del sistema de cómputo, ¿existe equipo capaces que soportar el trabajo?	X		
25	¿El SGBD tiene capacidad de teleproceso?		X	
26	Se ha investigado si ese tiempo de respuesta satisface a los usuarios?			X
27	¿La capacidad de almacenamiento máximo de la BD es suficiente para atender el proceso por lotes y el proceso remoto?			X

Entrevista 2-2

Elaboro: _____ Vo. Bo. Del Responsable: _____

Nombre Y Firma Nombre y Firma

Auditoria de Base de Datos:
Para hallar el SI
27 - 100%
19 - X
X = 70.37

Para hallar el NO
27 - 100%
5 - X
X = 18.52

5.8.1 INFORME DE AUDITORIA DE BASE DE DATOS

1. Identificación del informe

Auditoria de Base de Datos.

2. Identificación del Cliente

El área de Informática

3. Identificación de la Entidad Auditada

Área de Informática del comisariato de la Policía Nacional en Masaya.

4. Objetivos

- ✓ Evaluar el tipo de Base de Datos, relaciones, plataforma o sistema operativo que trabaja, llaves, administración y demás aspectos que repercuten en su trabajo.
- ✓ Revisar del software institucional para la administración de la Base de Datos.
- ✓ Verificar la actualización de la Base de Datos.
- ✓ Verificar la optimización de almacenes de los Base de Datos
- ✓ Revisar que el equipo utilizado tiene suficiente poder de procesamiento y velocidad en red para optimizar el desempeño de la base de datos.

5. Hallazgos Potenciales

- ♦ No están definidos los parámetros o normas de calidad.
- ♦ Falta de presupuesto
- ♦ Falta de personal
- ♦ La gerencia de Base de datos no tiene un plan que permite modificar en forma oportuna el plan a largo plazo de tecnología, teniendo en cuenta los posibles cambios tecnológicos y el incremento de la base de datos.
- ♦ No existe un calendario de mantenimiento de rutina periódico del software definido por la Base de datos.

6. Alcance de la auditoria

Nuestra auditoria, comprende el presente periodo 2014 y se ha realizado especialmente al Departamento de centro de informática de acuerdo a las normas y demás disposiciones aplicable al efecto.

7. Conclusiones:

- Como resultado de la Auditoria podemos manifestar que hemos cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoria
  .
- El Departamento de centro de informática presenta deficiencias sobre todo en el debido cumplimiento de Normas de seguridad de datos y administración de la Base de Datos.

8. Recomendaciones

- Elaborar toda la documentación lógica correspondiente a los sistemas de administración de la BD. Evaluar e implementar un software que permita mantener el resguardo de acceso de los archivos de programas y aún de los programadores.
- Implementar las relaciones con las diferentes áreas en cuanto al compartimiento de archivos permitidos por las normas
- Elaborar un calendario de mantenimiento de rutina periódico.
- Capacitar al personal al manejo de la BD.
- Dar a conocer la importancia del SGBD al usuario

9. Fecha Del Informe

	PLANEAMIENTO	**EJECUCIÓN**	**INFORME**
FECHA			

10. Identificación Y Firma Del Auditor

APELLIDOS Y NOMBRES	**CARGO**

5.9 AUDITORIA DE CALIDAD

Objetivos:

- Verificar los procesos aplicables del programa de la calidad ha sido desarrollado y documentados.
- Evaluar la capacidad de realizar un trabajo específico.

A03 Supervisión de la Integración del Expediente del Auditor

Dependencia:				
Área Auditada:				
Tipo de Auditoria:	**Número de Auditoria:**			
Fecha de Inicio:	**Fecha de Término:**			
Periodo Auditado:				
Personal Participante:				
	PREGUNTAS	**SI**	**NO**	**N/A**
1	¿Se reflejan el software codificado tal como en el diseño en la documentación?		X	
2	¿Fueron probados con éxito los productos de software usados en el centro de informática?	X		
3	¿Se cumplen las especificaciones de la documentación del usuario del software?	X		
4	¿Los procesos de gestión administrativa aplicados en el área de informática de la institución son lo suficientemente óptimos?		X	
5	¿El funcionamiento del software dentro del área de trabajo está de acuerdo con los requerimientos específicos?	X		
6	¿Los documentos de gestión administrativa se cumplen satisfactoriamente en el área de informática?		X	
7	¿Los productos de software que utilizan en el área de informática esta de acuerdo con los estándares establecidos?	X		
8	¿Los dispositivos de trabajo en el área de informática se les realizan una revisión técnica correcta?	X		
9	¿Los costos fijados en la revisión técnica se encuentran dentro de los límites fijados?		X	

Elaboro: _____ Vo. Bo. Del Responsable: _____

Nombre Y Firma Nombre y Firma

Auditoria Calidad:

Para hallar el SI

9 - 100%

5 - X

X = 55.5

Para hallar el NO

9 - 100%

4 - X

X = **44.4**

5.9.1 INFORME DE AUDITORIA DE CALIDAD

1. Identificación del informe

Auditoria de Calidad

2. Identificación del Cliente

El área de Informática

3. Identificación de la Entidad Auditada

Área Informática del comisariato de la Policía Nacional.

4. Objetivos

- Verificar la calidad de servicio que ofrece el Software.
- Evaluar el software institucional para la administración.
- Revisar que el equipo utilizado tiene suficiente poder de procesamiento y velocidad en red para optimizar el desempeño de la organización.

5. Alcance de la auditoria

Nuestra auditoria, comprende el presente periodo 2014 y se ha realizado especialmente al Departamento de centro de informática de acuerdo a las normas y demás disposiciones aplicable al efecto.

6. Conclusiones:

El Departamento de centro de informática presenta deficiencias sobre todo en el debido cumplimiento de Normas de seguridad de datos y administración de la
Base de Datos con respecto a calidad.

7. Fecha Del Informe

	PLANEAMIENTO	EJECUCIÓN	INFORME
FECHA			

8. Identificación Y Firma Del Auditor

APELLIDOS Y NOMBRES	CARGO

5.10 AUDITORIA DE LA SEGURIDAD

1. Alcance de la Auditoria.-

- Organización y calificación del personal
- Planes y procedimientos
- Sistemas técnicos de detección y comunicación
- Análisis de puestos
- Mantenimiento

2. Objetivos de la Auditoria.-

Realizar un informe de Auditoria con el objeto de verificar la adecuación de las medidas aplicadas a las amenazas definidas, así como el cumplimiento de los requisitos exigidos.

A03 Supervisión de la Integración del Expediente del Auditor

Auditoria de Seguridad del área lógica

Dependencia:				
Área Auditada:				
Tipo de Auditoria:	**Número de Auditoria:**			
Fecha de Inicio:	**Fecha de Término:**			
Periodo Auditado:				
Personal Participante:				
	PREGUNTAS	**SI**	**NO**	**N/A**
1	¿Existen medidas, controles, procedimientos, normas y estándares de seguridad?		X	
2	¿Existe un documento donde este especificado la relación de las funciones y obligaciones del personal?		X	
3	¿Existen procedimientos de notificación y gestión de incidencias?			X
4	¿Existen procedimientos de realización de copias de seguridad y de recuperación de datos?	X		
5	¿Existe una relación del personal autorizado a conceder, alterar o anular el acceso sobre datos y recursos?	X		
6	¿Existe una relación de controles periódicos a realizar para verificar el cumplimiento del documento?		X	
7	¿Existen medidas a adoptar cuando un soporte vaya a ser desechado o reutilizado?		X	
8	¿Existe una relación del personal autorizado a acceder a los locales donde se encuentren ubicados los sistemas que tratan datos personales?		X	

Entrevista 1-2

	PREGUNTAS	SI	NO	N/A
10	¿Existe un período máximo de vida de las contraseñas?	X		
11	¿Existe una relación de usuarios autorizados a acceder a los sistemas y que incluye los tipos de acceso permitidos?		X	
12	¿Los derechos de acceso concedidos a los usuarios son los necesarios y suficientes para el ejercicio de las funciones que tienen encomendadas, las cuales a su vez se encuentran o deben estar- documentadas en el Documento de Seguridad?		X	
13	¿Hay dadas de alta en el sistema cuentas de usuario genéricas, es decir, utilizadas por más de una persona, no permitiendo por tanto la identificación de la persona física que las ha utilizado?		X	
14	¿En la práctica las personas que tienen atribuciones y privilegios dentro del sistema para conceder derechos de acceso son las autorizadas e incluidas en el Documento de Seguridad?			X
15	¿El sistema de autenticación de usuarios guarda las contraseñas encriptadas?	X		
16	¿En el sistema están habilitadas para todas las cuentas de usuario las opciones que permiten establecer: • Un número máximo de intentos de conexión. • Un período máximo de vigencia para la contraseña, coincidente con el establecido en el Documento de Seguridad.	X		
17	¿Existen procedimientos de asignación y distribución de contraseñas?	X		

Entrevista 2-2

Elaboro: _____ Vo. Bo. Del Responsable: _____

Nombre Y Firma Nombre y Firma

A03 Supervisión de la Integración del Expediente del Auditor

Auditoria de Seguridad del área Física

Dependencia:				
Área Auditada:				
Tipo de Auditoria:	**Número de Auditoria:**			
Fecha de Inicio:	**Fecha de Término:**			
Periodo Auditado:				
Personal Participante:				
	PREGUNTAS	**SI**	**NO**	**N/A**
1	¿Existen procedimientos para la realización de las copias de Seguridad?	X		
2	¿Existen procedimientos que aseguran que, de todos los ficheros con datos de carácter personal, se realiza copia al menos una vez cada semana?		X	
3	¿Hay procedimientos que aseguran la realización de copias de todos aquellos ficheros que han experimentado algún cambio en su contenido?		X	
4	¿Existen controles para la detección de incidencias en la realización de las pruebas?		X	
5	¿Existen controles sobre el acceso físico a las copias de seguridad?	X		
6	¿Sólo las personas con acceso autorizado en el documento de seguridad tienen acceso a los soportes que contienen las copias de seguridad?		X	
7	¿Las copias de seguridad de ficheros de nivel alto incluyen los ficheros cifrados, si estas copias se transportan fuera de las instalaciones?			X
8	¿Las copias de seguridad de ficheros de nivel alto incluyen los ficheros cifrados, si estas copias se transportan fuera de las instalaciones?	X		
9	¿Las copias de seguridad de los ficheros de nivel alto se almacenan en lugar diferente al de los equipos que las procesan?	X		
10	¿Existe un inventario de los soportes existentes?		X	
11	¿Dicho inventario incluye las copias de seguridad?			X
12	¿Las copias de seguridad, o cualquier otro soporte, se almacenan fuera de la instalación?		X	
13	¿Existen procedimientos de actualización de dicho inventario?	X		
14	¿Existen procedimientos de etiquetado e identificación del contenido de los soportes?		X	
15	¿Existen procedimientos en relación con la salida de soportes fuera de su almacenamiento habitual?	X		
16	¿Se evalúan los estándares de distribución y envío de estos soportes?		X	

Entrevista 1-3

	PREGUNTAS	SI	NO	N/A
18	¿Se Comprueba que todos los soportes incluidos en esa relación se encuentran también en el inventario de soportes mencionado anteriormente?			X
19	¿Se Obtiene una copia del Registro de Entrada y Salida de Soportes y se comprueba que en él se incluyen: Los soportes incluidos en la relación del punto anterior (y viceversa) Los desplazamientos de soportes al almacenamiento exterior (si existiera)	X		
20	¿Se Verifica que el Registro de Entrada y Salida refleja la información requerida por el Reglamento: a) Fecha y hora b) Emisor/Receptor c) Nº de soportes d) Tipo de información contenida en el soporte. e) Forma de envío f) Persona física responsable de la recepción/entrega	X		
21	¿Se Analiza los procedimientos de actualización del Registro de Entrada y Salida en relación con el movimiento de soportes?		X	
22	¿Existen controles para detectar la existencia de soportes recibidos/enviados que no se inscriben en el Registro de Entrada/Salida?	X		
23	¿Se Comprueba, en el caso de que el Inventario de Soportes y/o el Registro de Entrada/Salida estén informatizados, que se realizan copias de seguridad de ellos, al menos, una vez a la semana?			X
24	¿Se realiza una relación de soportes enviados fuera de la empresa con la relación de ficheros de nivel alto?			X
25	¿Se Verifica que todos los soportes que contiene ficheros con datos de nivel Alto van cifrados?		X	
26	¿Se Comprobar la existencia, como parte del Documento de Seguridad, de una relación de usuarios con acceso autorizado a la sala?		X	
27	¿Se Verifica que la inclusión del personal en la relación anterior es coherente con las funciones que tienen encomendadas?			X
28	¿Se Comprueba que la relación es “lógica” (¿personal de limpieza? ¿Vigilantes de seguridad?).			X
29	¿Existen políticas de la instalación en relación con los accesos ocasionales a la sala?		X	
30	¿Se Determina que personas tienen llaves de acceso, tarjetas, etc. de acceso a la sala?			X
31	¿Se Comprueba que están activados los parámetros de activación del Registro para todos los ficheros de Nivel Alto?			X

Entrevista 2-2

	PREGUNTAS	SI	NO	N/A
33	¿Existen procedimientos de realización de copias de seguridad del Registro de Accesos y el período de retención de las copias?		X	
34	¿Se Verifica la asignación de privilegios que permitan activar/desactivar el Registro de Accesos para uno o más ficheros?	X		
35	¿Se Comprueba que el Registro de Accesos se encuentra bajo el control directo del Responsable de Seguridad pertinente?	X		

Entrevista 3-3

Elaboro: _____ Vo. Bo. Del Responsable: _____

Nombre Y Firma Nombre y Firma

Auditoria de Seguridad:

Para hallar el SI

52 - 100%

17 - X

X = 32.69

Para hallar el NO

52 - 100%

14 - X

X = **26.92**

AREAS CRÍTICAS DE LA AUDITORIA DE SEGURIDAD

Evaluación de la seguridad en el acceso al Sistema

Preguntas	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Evaluar los atributos de acceso al sistema.					X
Evaluar los niveles de acceso al sistema.			X		
Evaluar la administración de contraseñas al sistema				X	
Evaluar el monitoreo en el acceso al sistema.					X
Evaluar las funciones del administrador del acceso al sistema.				X	
Evaluar las medidas preventivas o correctivas en caso de siniestros n el acceso.			X		

Evaluación de la seguridad en el acceso al Área Física

Preguntas	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Evaluar el acceso del personal al centro de informática		X			
Evaluar el acceso de los usuarios y terceros al centro de informática.				X	
Evaluar el control de entradas ysalidas de bienes informáticos del centro de informática				X	
Evaluar la vigilancia del centro de cómputo					X
Evaluar las medidas preventivas o correctivas en caso de siniestro en el centro de informática				X	
Analizar las políticas de la instalación en relación con los accesos ocasionales a la sala.			X		

Evaluación de los planes de contingencias informáticos

Preguntas	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Evaluar la existencia, difusión, aplicación y uso de contra contingencias de sistemas.				X	
Evaluar la aplicación de simulacros, así como el plan contra contingencias.					X
Evaluar la confidencialidad, veracidad y oportunidad en la aplicación de las medidas del plan contra contingencias.			X		

Evaluación de la seguridad en los sistemas computacionales

Preguntas	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Evaluar el rendimiento y uso del sistema computacional y de sus periféricos asociados.			X		
Evaluar la existencia, protección y periodicidad de los respaldos debases de datos, software e información importante de la organización.				X	
Evaluar la configuración, instalaciones y seguridad del equipo de cómputo, mobiliario y demás equipos.				X	
Evaluar el rendimiento, aplicación y utilidad del equipo de cómputo, mobiliario y demás equipos.			X		
Evaluar la seguridad en el procesamiento de información.				X	
Evaluar los procedimientos de captura, procesamiento de datos y emisión de resultados de los sistemas computacionales.					X

Evaluación de la protección contra la piratería y robo de información

Preguntas	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Medidas preventivas.		X			
Protección de archivos.			X		
Limitación de accesos.					X
Protección contra robos				X	
Protección ante copias ilegales		X			

Evaluación de la protección contra virus informáticos

Preguntas	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Medidas preventivas y correctivas.			X		
Uso de vacunas y buscadores de virus.				X	
Protección de archivos, programas e información.				X	

Evaluación de la seguridad del hardware

Preguntas	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Realización de inventarios de hardware, equipos y periféricos asociados.			X		
Evaluar la configuración del equipo de computo (hardware).				X	
Evaluar el rendimiento y uso del sistema computacional y sus periféricos asociados.					X
Evaluar el estado físico del hardware, periféricos y equipos asociados				X	

Evaluación de la seguridad del Software

Preguntas	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Realización de inventarios de software, paqueterías y desarrollos empresariales.				X	
Evaluar las licencias permisos y usos de los sistemas computacionales.			X		
Evaluar el rendimiento y uso del software de los sistemas computacionales.					X
Verificar que la instalación del software, paqueterías y sistemas desarrollados en la empresa sea la adecuada para cubrir las necesidades de esta última.				X	

5.10.1 INFORME DE AUDITORIA DE SEGURIDAD FISICA

1. Identificación del informe

Auditoria de la Seguridad

2. Identificación del Cliente

El área de Informática

3. Identificación de la Entidad Auditada

Área de Informática del Comisariato de la Policía Nacional

4. Objetivos

- Hacer un estudio cuidadoso de los riesgos potenciales a los que está sometida el área de informática.
- Revisar tanto la seguridad física del Centro de Proceso de Datos en su sentido más amplio, como la seguridad lógica de datos, procesos y funciones informáticas más Importantes de aquél.

5. Hallazgos Potenciales

- No existe documentaciones técnicas del sistema integrado de la Cooperativa y tampoco no existe un control o registro formal de las modificaciones efectuadas.
- No se cuenta con un Software que permita la seguridad de las librerías de los programas y la restricción y/o control del acceso de los mismos.
- Las modificaciones a los programas son solicitadas generalmente sin notas internas, en donde se describen los cambios o modificaciones que se requieren.
- Falta de planes y Programas Informáticos.
- Poca identificación del personal con la institución
- Inestabilidad laboral del personal
- No existen programas de capacitación y actualización al personal

6. Alcance de la auditoria

Nuestra auditoria, comprende el presente periodo 2014 y se ha realizado especialmente al área de Informática de acuerdo a las normas y demás disposiciones aplicable al efecto.

7. Conclusiones:

- Como resultado de la Auditoria de la Seguridad realizada al CPN Masaya, por el período comprendido entre el 02 de enero al 31 de diciembre del 2014, podemos manifestar que hemos cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoria.
- El área de Informática presenta deficiencias sobre todo en el debido cumplimiento de sus funciones y por la falta de ellos.

8. Recomendaciones

- Elaborar toda la documentación técnica correspondiente a los sistemas implementados y establecer normas y procedimientos para los desarrollos y su actualización.
- Evaluar e implementar un software que permita mantener el resguardo de acceso de los archivos de programas y aún de los programadores.
- Implementar y conservar todas las documentaciones de prueba de los sistemas, como así también las modificaciones y aprobaciones de programas realizadas por los usuarios
- El coste de la seguridad debe considerarse como un coste más entre todos los que son necesarios para desempeñar la actividad que es el objeto de la existencia de la entidad, sea ésta la obtención de un beneficio o la prestación de un servicio público.
- El coste de la seguridad, como el coste de la calidad, son los costes de funciones imprescindibles para desarrollar la actividad adecuadamente.

9. Fecha Del Informe

	PLANEAMIENTO	**EJECUCIÓN**	**INFORME**
FECHA			

10. Identificación Y Firma Del Auditor

APELLIDOS Y NOMBRES	**CARGO**

5.11 AUDITORIA A LOS SISTEMAS DE REDES

1. Objetivos de la Auditoria.-

Realizar un informe de Auditoria con el objeto de verificar la adecuación de las medidas aplicadas a las amenazas definidas, así como el cumplimiento de los requisitos exigidos.

A03 Supervisión de la Integración del Expediente del Auditor

Dependencia:				
Área Auditada:				
Tipo de Auditoria:	**Número de Auditoria:**			
Fecha de Inicio:	**Fecha de Término:**			
Periodo Auditado:				
Personal Participante:				
	PREGUNTAS	**SI**	**NO**	**N/A**
1	La gerencia de redes tiene una política definida de planeamiento de tecnología de red?	X		
2	Esta política es acorde con el plan de calidad de la organización		X	
3	La gerencia de redes tiene un plan que permite modificar en forma oportuna el plan a largo plazo de tecnología de redes, teniendo en cuenta los posibles cambios tecnológicos o en la organización?		X	
4	Existe un inventario de equipos y software asociados a las redes de datos?	X		
5	Existe un plan de infraestructura de redes?	X		
6	El plan de compras de hardware y software para el sector redes está de acuerdo con el plan de infraestructura de redes?		X	
7	La responsabilidad operativa de las redes está separada de las de operaciones del computador?		X	
8	Están establecidos controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados		X	
9	Existen controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas?		X	
10	Existen controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red?		X	
11	Existen protocolos de comunicaron establecida	X		
12	Existe una topología estandarizada en toda la organización		X	
13	Existen normas que detallan que estándares que deben cumplir el hardware y el software de tecnología de redes?	X		
14	¿La transmisión de la información en las redes es segura?	X		
15	¿El acceso a la red tiene password?	X		

Elaboro: _____ Vo. Bo. Del Responsable: _____

Nombre Y Firma Nombre y Firma

AREA CRITICA REDES
LISTADO DE VERIFICACIÓN DE AUDITORIA DE REDES

Gestión Administrativa de la Red

	100% Excelente	**80% Buena**	**60% Regular**	**40% Mínimo**	**20% No cumple**
Los objetivos de la Red e computo Las características de la Red de computo				**X**	
Los componentes Físicos de la red de computo			**X**		
La conectividad y Las comunicaciones de la red decomputo			**X**	**X**	
Los servicios que proporcionan. La red de computo				**X**	
Las configuraciones , topologías , tipos Y cobertura de las redes de computo.			**X**		
Los protocolos de Comunicación interna de la red.				**X**	
La administración de la red de Cómputo.			**X**		

Análisis de los estudios de viabilidad y factibilidad en el diseño e instalación de la red de cómputo en la empresa:

Evaluar y calificar el cumplimiento de los siguientes aspectos	**100% Excelente**	**80% Buena**	**60% Regular**	**40% Mínimo**	**20% No cumple**
El estudio de factibilidad tecnológica		**X**			
El estudio factibilidad económica		**X**			
El estudio de factibilidad administrativa			**X**		
El estudio de factibilidad operativa			**X**		

Evaluación de análisis de la red de cómputo

Evaluar y calificar el cumplimiento de los siguientes aspectos	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
Evaluación de la existencia y uso de metodologías, normas, estándares y políticas para el análisis y diseño de redes de cómputo.				**X**	
Análisis de la definición de la problemática y solución para instalar redes de cómputo en la empresa.			**X**		
Análisis de cumplimiento de los objetivos fundamentales de la organización para instalar una red de computo, evaluando en cada caso.			**X**		
La forma de repartir los recursos informáticos de la organización, especialmente la información y los activos.			**X**		
La cobertura de servicios informáticos para la captura, el procesamiento y la emisión de información en la organización.				**X**	
La cobertura de los servicios de comunicación.			**X**	**X**	
La frecuencia con que los usuarios recurren a los recursos de la red.		**X**			
La confiabilidad y seguridades el uso de la información institucional.			**X**		
La centralización, administración, operación asignación y el control de los recursos informáticos de la organización.			**X**		
La distribución equitativa de los costos de adquisición y el control de los recursos informáticos de la organización.				**X**	
La escalabilidad y migración de los recursos computacionales de la organización				**X**	
La satisfacción de las necesidades de poder computacional de la Organización, sea con redes, cliente/servidor o mainframe.			**X**		
La solución a los problemas de comunicación de información y datos en las áreas de la organización.			**X**		

Evaluación del diseño e implementación de la red según el ámbito de cobertura.

	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
Análisis de las redes de multicomputadoras			**X**		
Evaluar el funcionamiento de la cobertura de punto a punto.		**X**			
Evaluar el funcionamiento de la tecnología que se usa con un solo cable entre las máquinas conectadas		**X**			
Evaluar el funcionamiento de las aplicaciones, usos y explotación de las redes			**X**		

Análisis de la red de área local (L A N)

	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
Evaluar el uso adecuado y confiable de la tecnología utilizada internamente para la transmisión de datos.			**X**		
Evaluar la restricción Adoptada para establecer el tamaño de la red.			**X**		
Evaluar la velocidad.		**X**			

5.11.1 Informe de Auditoria de redes.

1. Identificación del informe

Auditoria del Sistema de Redes

2. Identificación del Cliente

El área de Informática

3. Identificación de la Entidad Auditada

Comisariato de la Policía Nacional Masaya.

4. Objetivos

- Evaluar el tipo de red, arquitectura topología, protocolos de comunicación, las conexiones, accesos privilegios, administración y demás aspectos que repercuten en su instalación.
- Revisión del software institucional para la administración de la red.

5. Hallazgos Potenciales

- No se cuenta con un Software que permita la seguridad de restricción y/o control a la Red.

- No existe un plan que asegure acciones correctivas asociadas a la conexión con redes externas.
- No están definidos los parámetros o normas de calidad.
- La gerencia de redes no tiene un plan que permite modificar en forma oportuna el plan a largo plazo de tecnología de redes ,teniendo en cuenta los posibles cambios tecnológicos.
- No existe un calendario de mantenimiento de rutina periódico del hardware definido por la gerencia de redes.
- No existe un plan proactivo de tareas a fin de anticipar los problemas y solucionarlos antes de que los mismos afecten el desempeño de la red

6. Alcance de la auditoria

Nuestra auditoria, comprende el presente periodo 2014 y se ha realizado especialmente al área de Informática de acuerdo a las normas y demás disposiciones aplicable al efecto.

7. Conclusiones:

- Como resultado de la Auditoria podemos manifestar que hemos cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoria.
- El área de Informática presenta deficiencias sobre todo en el debido cumplimiento de Normas de redes y funciones.

8. Recomendaciones

- Elaborar toda la documentación técnica correspondiente a los sistemas de redes. Evaluar e implementar un software que permita mantener el resguardo de acceso de los archivos de programas y aún de los programadores.
- Implementar un plan que permita modificar en forma oportuna el plan a largo plazo de tecnología de redes.
- Elaborar un calendario de mantenimiento de rutina periódico del hardware.

9. Fecha Del Informe

	PLANEAMIENTO	**EJECUCIÓN**	**INFORME**
FECHA			

10. Identificación Y Firma Del Auditor

APELLIDOS Y NOMBRES	**CARGO**

5.12 AUDITORIA DE APLICACIONES

1. Objetivos
Realizar un informe de Auditoria con el objeto de verificar la adecuación de los estándares de funcionamiento y procedimiento del área de informática.

A03 Supervisión de la Integración del Expediente del Auditor

Dependencia:				
Área Auditada:				
Tipo de Auditoria:	**Número de Auditoria:**			
Fecha de Inicio:	**Fecha de Término:**			
Periodo Auditado:				
Personal Participante:				
	PREGUNTAS	**SI**	**NO**	**N/A**
1	¿Existe una lista de proyectos de sistema de procedimiento de información y fechas programadas de implantación que puedan ser considerados como plan maestro?	X		
2	¿Está relacionado el plan maestro con un plan general de desarrollo de la dependencia?		X	
3	¿Ofrece el plan maestro la atención de solicitudes urgentes de los usuarios?		X	
4	¿Asigna el plan maestro un porcentaje del tiempo total de producción al reproceso o fallas de equipo?		X	
5	Existe la lista de proyectos a corto plazo y largo plazo X	X		
6	Existe una lista de sistemas en proceso periodicidad y usuarios	X		
7	Incluir el plazo estimado de acuerdo con los proyectos que se tienen en que el departamento de informática podría satisfacer las necesidades de la dependencia, según la situación actual	X		
8	¿Considera que el Departamento de Sistemas de Información de los resultados esperados?	X		
9	¿Existen fallas de exactitud en los procesos de información?	X		
10	¿Se cuenta con un manual de usuario por Sistema?		X	
11	¿Es claro y objetivo el manual del usuario?			X
12	¿Qué opinión tiene el manual?			X
13	¿Se interviene de su departamento en el diseño de sistemas?		X	

Elaboro: _____ Vo. Bo. Del Responsable: _____
Nombre Y Firma Nombre y Firma

Auditoria de Aplicaciones:

- **Para hallar el SI**

13 - 100%
6 - X
X = 46.15

- **Para hallar el NO**

13 - 100%
5 - X
X = **38.46**

5.12.1 INFORME DE AUDITORIA DE APLICACIONES.

1. Identificación del informe

Auditoria de Aplicaciones

2. Identificación del Cliente

El área de Informática

3. Objetivos

- ✓ Evaluar el papel del área de informática en la Institución
- ✓ Evaluar el plan estratégico del área de Informática.
- ✓ Evaluar la seguridad de los programas en el sentido de garantizar que los ejecutados por la maquina sean exactamente los previstos y no otros.
- ✓ Evaluar la existencia del plan operativo anual del área de Informática
- ✓ Verificar el cumplimiento de los objetivos, planes y presupuestos contenidos en el plan de sistemas de información.
- ✓ Evaluar el nivel de satisfacción de los usuarios del sistema.
- ✓ Verificar el grado de fiabilidad de la información.

4. Hallazgos Potenciales

- ✓ Incumplimiento de los plazos previstos en cada una de las fases del proyecto.
- ✓ Ineficacia e inseguridad del sistema de control de accesos diseñado.
- ✓ Falta de metodologías utilizadas que asegure la modularidad de las posibles futuras ampliaciones de la Aplicación y el fácil mantenimiento de las mismas.
- ✓ Incompatibilidad de las herramientas técnicas utilizadas en los diversos programas.
- ✓ Falta de sencillez, modularidad y economía de recursos del diseño de programas.

5. Alcance de la auditoria

Nuestra auditoria, comprende el presente periodo 2014 y se ha realizado especialmente al área de Informática de acuerdo a las normas y demás disposiciones aplicable al efecto.

6. Conclusiones:

- ✓ Como resultado de la Auditoria de Aplicaciones realizada en el CPN Masaya, por el período comprendido entre el 02 de enero al 31 de diciembre del 2014, podemos manifestar que hemos cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoria.
- ✓ El área de Informática presenta deficiencias sobre todo en la falta de metodologías que son necesarias al realizar un proyecto.

7. Recomendaciones

- ✓ Emplear metodologías que asegure la modularidad de las posibles futuras ampliaciones de la Aplicación y el fácil mantenimiento de las mismas.
- ✓ Realizar un control Interno de las Aplicaciones, verificando que las mismas fases se utilicen en el área correspondiente de Desarrollo
- ✓ Hacer un estudio de Vialidad de la Aplicación sobre todo para aquellas que son largas complejas y caras.
- ✓ Utilizar herramientas técnicas compatibles
- ✓ Capacitar al personal para el diseño de Programas para realizarlos con la máxima sencillez, modularidad y economía de recursos

8. Fecha Del Informe

	PLANEAMIENTO	**EJECUCIÓN**	**INFORME**
FECHA			

9. Identificación Y Firma Del Auditor

APELLIDOS Y NOMBRES	**CARGO**

5.13 Auditoria física

1. Alcance de la auditoria

- ✓ Organización y cualificación del personal de seguridad.
- ✓ Remodelar el ambiente de trabajo.
- ✓ Planes y procedimientos.
- ✓ Sistemas técnicos de seguridad y protección.

2. Objetivos

- ✓ Revisión de las políticas y normas sobre seguridad física.
- ✓ Verificar la seguridad del personal, datos, hardware, software e instalaciones.
- ✓ Seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático.

A03 Supervisión de la Integración del Expediente del Auditor

Dependencia:	
Área Auditada:	
Tipo de Auditoria:	**Número de Auditoria:**
Fecha de Inicio:	**Fecha de Término:**
Periodo Auditado:	
Personal Participante:	

	Preguntas	Si	No	N/A
1.	¿Se han adoptado medidas de seguridad en el departamento de sistemas de información ?		X	
2.	¿Existe una persona responsable de la seguridad		X	
3.	¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?		X	
4.	¿Existe personal de vigilancia en la empresa?	X		
5.	¿Existe una clara definición de funciones entre los puestos claves?		X	
6.	¿Se investigan a los vigilantes cuando son contratados ?		X	
7.	¿Se controla el trabajo fuera de horario?		X	
8.	¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas ?	X		
9.	¿Existe vigilancia en el departamento de computo las 24 horas?		X	
10.	¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?		X	

Entrevista 1-2

	Preguntas	Si	No	N/A
12.	¿El centro de computo tiene salida al exterior?		X	
13.	¿Son controladas las visitas y demostraciones en el centro de computo?	X		
14.	¿Se registra el acceso al departamento de computo las personas ajenas a la dirección de informática ?	X		
15.	¿Se vigilan la moral y comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar un posible fraude ?		X	
16.	¿Se ha adiestrado al personal en el manejo de extintores?		X	
17.	¿ Si es que existen extintores automáticos son activados por detectores automáticos de fuego?		X	
18.	¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?		X	
19.	¿Saben que hacer los operadores del departamento de computo, en caso de que ocurra una emergencia ocasionada por fuego?	X		
20.	¿Existe salida de emergencia ?	X		
21.	¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de computo para evitar daños al equipo?	X		
22.	¿Se cuenta con copias de los archivos en un lugar distinto al de la computadora?		X	
23.	¿Se tienen establecidos procedimientos de actualización a estas copias ?		X	
24.	¿ Existe departamento de auditoría interna en la empresa?	X		
25.	¿ Este departamento de auditoría interna conoce todo los aspectos de los sistemas ?		X	
26.	¿ Se auditan los sistemas en operación?		X	
27.	Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?	X		
28.	¿Existe control estricto en las modificaciones ?	X		
29.	¿ Si se tienen terminales conectadas ¿ se ha establecido procedimientos de operación ?		X	
30.	¿Se ha establecido que información puede ser acezada y porque persona?		X	

Entrevista 2-2

LISTADO DE VERIFICACIÓN DE AUDITORIA FISICA

Gestión física de seguridad

	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Los objetivos de la instalación física de computo					X
Las características físicas de son seguras de centro				X	
Los componentes físicos de computo son completos		X			
Las conexiones de los equipos de las comunicaciones e instalaciones físicas.			X		

Evaluación de análisis física de cómputo

	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Evaluación de la existencia y uso de normas, resolución base legal para el diseño del centro de informática.					X
El cumplimiento de los objetivos fundamentales de la organización para instalar del centro de informática.					X
La forma de repartir los recursos informáticos de la organización.					X
La confiabilidad y seguridades el uso de la información empresa				X	
La satisfacción de las necesidades de poder computacional de la organización.				X	
La solución a identificación del centro de informática		X			

Análisis de la delimitación la manera en que se cumplen:

	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
La delimitación espacial, por las dimensiones físicas.					X
La delimitación tecnológica, por los requerimientos y conocimientos informáticos.				X	

Análisis de la estabilidad y el aprovechamiento de los recursos a para instalar el centro de informática.

	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No Cumple
Análisis de la transparencia del trabajo para los usuarios.			X		
La ubicación del centro de computo					
Los requerimientos de seguridad del centro de computo				X	

Evaluación del diseño según el ámbito.

	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No Cumple
Análisis del ambiente de Trabajo				X	
Evaluar el funcionamiento de los equipos			X		
Los equipos cuentan con Ventilación		X			

5.13.1 INFORME DE AUDITORIA FISICA.

1. Identificación del informe

Auditoria física.

2. Identificación del Cliente

El área de Informática

3. Identificación de la Entidad Auditada

Comisariato de la Policía Nacional en Masaya.

4. Objetivos

- ✓ Verificar la estructura de distribución de los equipos.
- ✓ Revisar la correcta utilización de los equipos
- ✓ Verificar la condición del centro de Informática.

5. Hallazgos Potenciales

- ♦ Falta de presupuesto y personal.
- ♦ Falta de un local más amplio
- ♦ No existe un calendario de mantenimiento
- ♦ Falta de ventilación.
- ♦ Faltan salida al exterior
- ♦ No existe salidas de emergencia.

6. Alcance de la auditoria

Nuestra auditoria, comprende el presente periodo 2014 y se ha realizado especialmente al Departamento de informática de acuerdo a las normas y demás disposiciones aplicable al efecto.

7. Conclusiones:

- Como resultado de la Auditoria podemos manifestar que hemos cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoría.

- El Departamento de informática presenta deficiencias sobre todo en el debido cumplimiento de Normas de seguridad.

8. Recomendaciones

- Reubicación del local
- Implantación de equipos de última generación
- Implantar equipos de ventilación
- Implantar salidas de emergencia.
- Elaborar un calendario de mantenimiento de rutina periódico.
- Capacitar al personal.

9. Fecha Del Informe

	PLANEAMIENTO	**EJECUCIÓN**	**INFORME**
FECHA			

10. Identificación Y Firma Del Auditor

APELLIDOS Y NOMBRES	**CARGO**

5.14 Auditoria de la dirección

1. **Alcance de la Auditoria.**

- ✓ Organización y calificación de la dirección de Informática
- ✓ Plan Estratégico de Sistemas de Información.
- ✓ Análisis de puestos
- ✓ Planes y Procedimientos
- ✓ Normativa
- ✓ Gestión Económica.

2. Objetivos de la Auditoria.-

Realizar un informe de Auditoría con el objeto de verificar la adecuación de las medidas aplicadas a las amenazas definidas, así como el cumplimiento de los requisitos exigidos.

3. **Resultados**: Se obtendrá:
   - Informe de Auditoría detectando riesgos y deficiencias en la Dirección de Informática.
   - Plan de recomendaciones a aplicar en función de:
     - Normativa a cumplir.
     -

A03 Supervisión de la Integración del Expediente del Auditor

Dependencia:	
Área Auditada:	
Tipo de Auditoria:	**Número de Auditoria:**
Fecha de Inicio:	**Fecha de Término:**
Periodo Auditado:	
Personal Participante:	

PREGUNTAS	SI	NO	N/A
1. ¿La dirección de los servicios de información desarrollan regularmente planes a corto, medio y largo plazo que apoyen el logro de la misión y las metas generales de la organización?	X		
2. ¿Dispone su institución de un plan Estratégico de Tecnología de Información?	X		
3. ¿Durante el proceso de planificación, se presta adecuada atención al plan estratégico de la empresa?	X		
4. ¿Las tareas y actividades en el plan tiene la correspondiente y adecuada asignación de recursos?		X	
5. ¿Existe un comité de informática?			X

Entrevista 1-2

PREGUNTAS	SI	NO	N/A
7. ¿Existen estándares de funcionamiento y procedimientos y descripciones de puestos de trabajo adecuados y actualizados?		X	
8. ¿Los estándares y procedimientos existentes promueven una filosofía adecuada de control?	X		
9. ¿Las descripciones de los puestos de trabajo reflejan las actividades realizadas en la práctica?	X		
10. ¿La selección de personal se basa en criterios objetivos y tiene en cuenta la formación, experiencia y niveles de responsabilidad?	X		
11. ¿El rendimiento de cada empleado se evalúa regularmente en base a estándares establecidos?	X		
12. ¿Existen procesos para determinar las necesidades de formación de los empleados en base a su experiencia?	X		
13. ¿Existen controles que tienden a asegurar que el cambio de puesto de trabajo y la finalización de los contratos laborales no afectan a los controles internos y a la seguridad informática?	X		
14. ¿Existe un presupuesto económico? ¿Y hay un proceso para elaborarlo?	X		
15. ¿Existen procedimientos para la adquisición de bienes y servicios?	X		
16. ¿Existe un plan operativo anual?	X		
17. ¿Existe un sistema de reparto de costes informáticos y que este sea justo?		X	
18. ¿Cuentan con pólizas de seguros?	X		
19. ¿Existen procedimientos para vigilar y determinar permanentemente la legislación aplicable?			X

Entrevista 2-2

5.15 Auditoria de explotación

A03 Supervisión de la Integración del Expediente del Auditor

Dependencia:	
Área Auditada:	
Tipo de Auditoria:	**Número de Auditoria:**
Fecha de Inicio:	**Fecha de Término:**
Personal Participante:	

1.	¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, al personal autorizado?	X		
2.	¿Se tiene relación del personal autorizado para firmar la salida de archivos confidenciales?		X	
3.	¿Existe un procedimiento para registrar los archivos que se prestan y la fecha en que se devolverán?	X		
4.	¿Se lleva control sobre los archivos prestados por la instalación?			X
5.	¿Se conserva la cinta maestra anterior hasta después de la nueva cinta?	X		
6.	¿El cintotecario controla la cinta maestra anterior previendo su uso incorrecto o su eliminación prematura?	X		
7.	¿La operación de reemplazo es controlada por el cintotecario?	X		
8.	¿Se utiliza la política de conservación de archivos hijo-padre abuelo?	X		
9.	En los procesos que manejan archivos en línea, ¿Existen procedimientos para recuperar los archivos?	X		
10.	¿Estos procedimientos los conocen los operadores?		X	
11.	¿Existe un responsable en caso de falla?			
12	¿Existen políticas que siguen para la obtención de archivos de respaldo?	X		
13.	¿Existe un procedimiento para el manejo de la información de la cintoteca?		X	
14.	¿Lo conoce y lo sigue el cintotecario?			X
15.	¿Existe un programa de trabajo de captación de datos?		X	
16.	¿Se controla las entradas de documentos fuente?	X		
17.	¿Existen documento de entrada se tienen? Sistemas documento del Dpto. que periodicidad Observaciones proporciona el documento		X	
18.	¿Se anota que persona recibe la información y su volumen?		X	
19.	¿Se anota a que capturista se entrega la información, el volumen y la hora?		X	

5.15.1 INFORME DE AUDITORIA DE EXPLOTACIÓN.

1. Identificación del informe

Auditoria de la Explotación

2. Identificación del Cliente

El área de Informática

3. Identificación de la Entidad Auditada

Comisariato de la Policía Nacional de Masaya

4. Objetivos

- Verificar el cumplimiento de plazos y calendarios de tratamientos y entrega de datos; la correcta transmisión de datos entre entornos diferentes.

- Verificar la existencia de normas generales escritas para el personal de explotación en lo que se refiere a sus funciones.

- Verificar la realización de muestreos selectivos de la Documentación de las Aplicaciones explotadas.

- Evaluar las relaciones personales y la coherencia de cargos y salarios, así como la equidad en la asignación de turnos de trabajo.

- Verificar la existencia de un responsable de Sala en cada turno de trabajo.

- Revisar la adecuación de los locales en que se almacenan cintas y discos, así como la perfecta y visible identificación de estos medios.

5. Hallazgos Potenciales

- Incumplimiento de plazos y calendarios de tratamientos y entrega de datos.
- Inexistencia y falta de uso de los Manuales de Operación.
- Falta de planes de formación.
- No existe programas de capacitación y actualización al personal.

6. Alcance de la auditoria

Nuestra auditoria, comprende el presente periodo 2014 y se ha realizado especialmente al área de Informática de acuerdo a las normas y demás disposiciones aplicable al efecto.

7. Conclusiones:

Como resultado de la Auditoria de la Seguridad realizada al Comisariato de la Policía nacional de Masaya por el período comprendido entre el 02 de enero al 31 de Diciembre del 2014, podemos manifestar que hemos cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoría. El área de Informática presenta deficiencias sobre todo en el debido cumplimiento de sus funciones y por la falta de ellos.

8. Recomendaciones

- Deberán realizarse muestreos selectivos de la documentación de las aplicaciones explotadas.
- Asignar un responsable del Centro de Cómputos en cada turno de trabajo.
- Crear y hacer uso de manuales de operación.
- Revisar los montajes diarios y por horas de cintas o cartuchos, así como los**.**
- Realizar funciones de operación, programación y diseño de sistemas deben
- estar claramente delimitadas.
- Crear mecanismos necesarios a fin de asegurar que los programadores y
- analistas no tengan acceso a la operación del computador y los operadores a
- su vez no conozcan la documentación de programas y sistemas.

9. Fecha Del Informe

	PLANEAMIENTO	**EJECUCIÓN**	**INFORME**
FECHA			

10. Identificación Y Firma Del Auditor

APELLIDOS Y NOMBRES	**CARGO**

5.16 AUDITORIA DEL DESARROLLO.

Dependencia:	
Área Auditada:	
Tipo de Auditoria:	**Número de Auditoria:**
Fecha de Inicio:	**Fecha de Término:**
Personal Participante:	

	Preguntas	Si	No	N/A
1.	¿Existe el documento que contiene las funciones que son competencia del área de desarrollo, está aprobado por la dirección de informática y se respeta?			
2.	¿Se comprueban los resultados con datos reales?			
3.	¿Existe un organigrama con la estructura de organización del área?			
4.	¿Existe un manual de organización que regula las relaciones entre puestos?			
5.	¿Están establecidos los procedimientos de promoción de personal a puestos superiores, teniendo en cuenta la experiencia y formación?			
6.	¿El personal de área de desarrollo cuenta con la formación adecuada y son motivados para la realización de su trabajo?			
7.	¿Existen procedimientos de contratación?			
8.	¿Las personas seleccionadas cumplen los requisitos del puesto al que acceden?			
9.	¿Existe un plan de formación que este en consonancia con los objetivos tecnológicos que se tenga en el área?			
10.	¿En los abandonos del personal se garantiza la protección del área?			
11.	¿Existe una biblioteca y una hemeroteca accesibles por el personal del área?			

Entrevista 1-2.

	Preguntas	Si	No	N/A
12.	¿El personal está motivado en la realización de su trabajo?			
13.	¿Existe algún mecanismo que permita a los empleados hacer sugerencias sobre mejoras en la organización del área?			
14.	¿Existe rotación de personal y existe un buen ambiente de trabajo?			
15.	¿La realización de nuevos proyectos se basa en el plan de sistemas en cuanto a objetivos?			
16.	¿Las fechas de realización coinciden con los del plan de sistemas?			
17.	¿El plan de sistemas se actualiza con la información que se genera a lo largo de un proceso?			
18.	¿Existe un mecanismo para registrar necesidades de desarrollo de nuevos sistemas?			
19.	¿Se tiene implantada una metodología de desarrollo de sistemas de información soportada por herramientas de ayuda?			
20.	¿La metodología cubre todas las fases del desarrollo y es adaptable a las distintas necesidades?			

Entrevista 2- 2

5.16.1 INFORME DE AUDITORIA DE DESARROLLO.

1. Identificación del informe
Auditoria de Desarrollo

2. Identificación del Cliente

El área de Informática

3. Identificación de la Entidad Auditada

Comisariato de la Policía Nacional en Masaya.

4. Objetivos

- Revisar el cumplimiento de las normas generales.
- Revisar los recursos de la organización.
- Verificar los avances tecnológicos.

5. Hallazgos Potenciales

- Incumplimiento de plazos y calendarios de tratamientos y entrega de datos
- Inexistencia y falta de uso de los Manuales de Operación
- Falta de planes de formación
- No existe programas de capacitación y actualización al personal

6. Alcance de la auditoria

Nuestra auditoria, comprende el presente periodo 2014 y se ha realizado especialmente al área de Informática de acuerdo a las normas y demás disposiciones aplicable al efecto.

7. Conclusiones:

- El Comisariato de la Policía Nacional en Masaya no desarrolla software de paliación si no la adquiere.
- Se calificado el ciclo de desarrollo de los procesos de la entidad en su ámbito de trabajo**.**

8. Recomendaciones

- Asignar un responsable un responsable para todos los procesos del Centro de
    - Informática.
- Se debe asignar un grupo para el desarrollo de software.
- Crear y hacer uso de manuales de operación.
- Realizar funciones de operación, diseño de sistemas.

5.17 AUDITORIA DE LA OFIMATICA.

Dependencia:	
Área Auditada:	
Tipo de Auditoria:	**Número de Auditoria:**
Fecha de Inicio:	**Fecha de Término:**
Personal Participante:	

	Preguntas	Si	No	N/A
1.	¿Existe un informe técnico en el que se justifique la adquisición del equipo, software y servicios de computación, incluyendo un estudio costo beneficio?			
2.	¿Existe un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación?			
3.	¿Han elaborado un instructivo con procedimientos a seguir para la selección y adquisición de equipos, programas y servicios computacionales?			
4.	¿Se cuenta con software de oficina?			
5.	¿Se ha asegurado un respaldo de mantenimiento y asistencia técnica?			
6.	¿El acceso al área de informática cuenta con las seguridades necesarias para reservar el ingreso al personal autorizado?			
7.	¿Se han implantado claves o password para garantizar operación de consola y equipo central a personal autorizado?			
8.	¿Se han formulado políticas respecto a seguridad, privacidad y protección de las facilidades de procesamiento ante eventos como: incendio, vandalismo, robo y uso indebido?			
9.	¿Se mantiene un registro permanente (bitácora) de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos.?			
10.	¿Los operadores del equipo central están entrenados para recuperar o restaurar información en caso de destrucción de archivos?			
11.	¿Los backups son mayores de dos (padres e hijos) y se guardan en lugares seguros y adecuados?			
12.	¿Se han implantado calendarios de operación a fin de establecer prioridades de proceso?			
13.	¿Todas las actividades del Centro de Computo están normadas mediante manuales, instructivos, normas, reglamentos, etc.?			

Entrevista 1-2

	Preguntas	Si	No	N/A
15.	¿Se han instalado equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de voltaje, supresores pico, UPS, generadores de energía?			
16.	¿Si se vence la garantía de mantenimiento del proveedor se contrata mantenimiento preventivo y correctivo?			
17.	¿Se han Adquirido equipos de protección como supresores de pico, reguladores de voltaje y de ser posible UPS previo a la adquisición del equipo.?			
18.	¿Se han contratado pólizas de seguros para proteger la información, equipos, personal y todo riesgo que se produzca por casos fortuitos o mala operación?			
19.	¿Se establecen procedimientos para obtención de backups de paquetes y de archivos de datos?			
20.	¿Se hacen revisiones periódicas y sorpresivas del contenido del disco para verificar la instalación de aplicaciones no relacionadas a la gestión de la empresa?			
21.	¿Se mantiene programas y procedimientos de detección e inmunización de virus en copias no autorizadas o datos procesados en otros equipos?			
22.	¿Se pretende a la estandarización del Sistema Operativo, software utilizado como procesadores de palabras, hojas electrónicas, manejadores de base de datos y se mantienen actualizadas las versiones y la capacitación sobre modificaciones incluidas?			
23.	¿existen licencias?			

Entrevista 2-2

5.17.1 INFORME DE AUDITORIA DE OFIMATICA.

1. Identificación del informe

Auditoria de la Ofimática

2. Identificación del Cliente

El área de Informática

3. Identificación de la Entidad Auditada

Comisariato de la Policía Nacional en Masaya

4. Objetivos

- Verificar si el hardware y software se adquieren siempre y cuando tengan la seguridad de que los sistemas computarizados proporcionaran mayores beneficios que cualquier otra alternativa.

- Verificar si la selección de equipos y sistemas de computación es adecuada

- Verificar que los procesos de compra de Tecnología de Información, deben estar sustentados en Políticas, Procedimientos, Reglamentos y Normatividad en general, que aseguren que todo el proceso se realiza en un marco de legalidad y cumpliendo con las verdaderas necesidades de la organización para hoy y el futuro, sin caer en omisiones, excesos o incumplimientos.

- Verificar si existen garantías para proteger la integridad de los recursos Informáticos.

- Verificar la utilización adecuada de equipos acorde a planes y objetivos.

- Verificar la existencia de un plan de actividades previo a la instalación

5. Hallazgos Potenciales

- Falta de licencias de software.
- Falta de software de aplicaciones actualizados.
- No existe un calendario de mantenimiento ofimático.
- Faltan material ofimática.
- Carece de seguridad en Acceso restringido de los equipos ofimático y software.

6. Alcance de la auditoria

Nuestra auditoria, comprende el presente periodo 2014 y se ha realizado al Departamento informática de acuerdo a las normas y demás disposiciones aplicable al efecto.

El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoria Ofimática, se complementa con los objetivos de ésta.

7. Conclusiones:

- Como resultado de la Auditoria podemos manifestar que hemos cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoría.

- El Departamento de centro de cómputo presenta deficiencias sobre el debido cumplimiento de Normas de seguridad.
- La escasez de personal debidamente capacitado.

- Cabe destacar que la sistema ofimático pudiera servir de gran apoyo de la empresa el cual no es explotado en su totalidad por falta de personal capacitado.

8. Recomendaciones

- Se recomienda contar con sellos y firmas digitales
- Un de manual de funciones para cada puesto de trabajo dentro del área.
- Reactualización de datos.
- Implantación de equipos de última generación
- Elaborar un calendario de mantenimiento de rutina periódico.
- Capacitar al personal

Comisariato de la Policía en Masaya

Proyecto: Auditoría Informática - Evaluación de la Situación Actual de los Servicios de Tecnología de Información
ESTRUCTURA ORGANIZACIONAL DEL AREA DE SISTEMAS (CONTROLES SOBRE LAS ACTIVIDADES IT)
Requerimiento: Estructura de Personal
Objetivo de Control COBIT: Definición de la Organización y de las Relaciones IT / PO4
Definición de la Organización y de las Relaciones IT – Segregación de Funciones. PO4
Procedimiento: Dependencia, Roles y Responsabilidades del personal del área informática
Evaluación de la segregación de funciones.

Trabajo realizado	Resultados Obtenidos	Debilidades identificadas	Nivel de riesgo	Recomendación	Prioridad
Entrevistas con los empleados	El comisariato de la Policía de Masaya cuenta con un departamento de sistemas, que son parte de los equipos de Administración de Redes, Administración de Bases de Datos, Soporte al usuario final y Mantenimiento de equipo electrónico, cuyo principal objetivo es asesorar y asistir técnicamente en lo correspondiente al campo tecnológico informático, y tiene asociados de negocios para áreas como las de desarrollo y renta de equipos de computación. El comisariato de la policía nacional de Masaya cuenta con un documento en el que se especifica de manera general las funciones de cada área sin embargo no existe un Manual de Funciones detallado para los miembros del departamento de Informática.	La Compañía no cuenta con un Manual de Funciones formalizado, en el que se detalle las tareas que debe realizar cada miembro del departamento de Informática.	Bajo	Elaborar el manual detallado para el comisariato de la policía de Masaya	Baja

Comisariato de la policía de Masaya.

Proyecto: Auditoría de Informática - Evaluación de la Situación Actual de los Servicios de Tecnología de Información

Trabajo realizado	Resultados obtenidos	Debilidades identificadas	Nivel de riesgo	Recomendaciones	Prioridad
Revisión con base a entrevistas de las funciones que cumple el personal de sistemas.	Existen actividades bajo la responsabilidad de sistemas y efectuados por su personal que no están acorde a sus funciones y responsabilidades.	Las funciones de Administración de Seguridades actualmente son realizadas por personal de Sistemas, lo cual no garantiza una adecuada segregación de funciones.	Alto	Redefinir la Estructura actual del Área de Informática, con el fin de optimizar los servicios que presta al Comisariato de la Policía en Masaya.	Alta
	El Comisariato de la policía en Masaya no cuenta con la función de auditoría informática	El Comisariato de la Policía en Masaya no existe una función de auditoría de informática	Medio	Implementar la función de Auditoría Informática, la cual supervisará las actividades del Administrador de Seguridades, y del área de Sistema en general	Media

Comisariato de la Policía en Masaya.
Proyecto: Auditoría de informática
Evaluación de la Situación Actual de los Servicios de Tecnología de Información
Requerimiento: Estructura de Personal
Objetivo de Control COBIT: Administración de Recursos Humanos / PO7
Procedimiento: Análisis del perfil de cada cargo tipo y sus ocupantes (experiencia, capacitación y escolaridad).

Trabajo realizado	Resultados obtenidos	Debilidades Identificadas	Nivel de Riesgo	Recomendación	Prioridad
Revisión de las hojas de vida de todo el personal de la Compañía. Análisis del perfil de cada empleado, nivel de experiencia y capacitación recibida.	El departamento de Recursos Humanos, nos proporcionó las hojas de vida del personal. Analizamos cada una de las hojas de vida , identificando lo siguiente: Un alto porcentaje del personal tiene experiencia previa a su contratación, ya que han trabajado en Compañías similares o han ejercido tareas similares a las que están ejecutando actualmente.				
	No existe un registro individual de la capacitación recibida. La mayoría del personal tienen experiencia previa a su ingreso. Recursos Humanos efectúa evaluaciones anuales de personal la cual considera muchos aspectos relacionados con el desempeño, evaluación y necesidades del empleado. Además se efectúan evaluaciones mensuales para determinar el porcentaje de cumplimiento de metas	El Comisariato de la Policía en Masaya no ha desarrollado un Plan de Capacitación Técnico para el próximo año, el mismo debería depender de las necesidades tecnológicas que tenga la empresa.	Bajo	Elaborar un plan formal de capacitación al personal	Baja

Comisariato de la Policía de Masaya.

Proyecto: Auditoría de Sistemas - Evaluación de la Situación Actual de los Servicios de Tecnología de Información
GESTION DE LOS SISTEMAS INFORMATICOS

Requerimiento: Desarrollo, Operación y Mantenimiento de Aplicaciones

Objetivo de Control COBIT: Administración de Calidad – Metodología del Ciclo de Vida de Desarrollo de Sistemas PO11
Procedimiento: Revisar y evaluar la metodología de desarrollo de aplicaciones existente.
Relevar los procedimientos para desarrollo de aplicaciones utilizados**.**

Trabajo realizado	Resultados obtenidos	Debilidades identificadas	Nivel de riesgo	Recomendación	Prioridad
Revisión de la Metodología y los procedimiento para desarrollo de aplicaciones	El comisariato de la policía en Masaya no posee una metodología formal para el desarrollo de aplicaciones, por cuanto no es una actividad significativa para la compañía, el soporte se lo solicita directamente a proveedores.	No existe un procedimiento formal para solicitud de nuevos requerimientos y/o modificaciones menores sobre las aplicaciones utilizadas. La priorización de requerimientos no son comunicados sistemática y formalmente a los usuarios involucrados.	Medio	Definir formalmente un procedimiento para la recepción y/o solicitud de requerimientos de usuarios relacionado con las aplicaciones utilizadas por la empresa, el procedimiento debe considerar la utilización de formularios, aprobaciones respectivas, así como, notificación a los usuarios de las prioridades asignadas a los requerimientos. Cambios a las prioridades deberán ser notificados a los usuarios involucrados.	Media

Comisariato de la Policía en Masaya.
Proyecto: Auditoría Informática
Objetivo de Control COBIT: Administración de proyectos /PO10
Instalación y Acreditación de Sistemas / AI5
Adquisición y Mantenimiento de Software de Aplicación / AI2

Procedimiento:

- Evaluar los procedimientos e iniciativas de investigación y desarrollo.
- Evaluar los procedimientos para pasar los programas de ambiente de desarrollo a producción.
- Revisar la documentación de la planificación de mantenimiento / mejora de aplicaciones así como la documentación que sustenta la prueba y otros procesos de recepción por parte del usuario**.**

Trabajo realizado	Resultados obtenidos	Debilidades identificadas	Nivel de riesgo	Recomendaciones	Prioridad
✓ Revisión de la metodología para el análisis y diseño de sistemas. ✓ Revisión de los procedimientos para el análisis y diseño de sistemas.	El comisariato de la policía en Masaya utiliza algunos lineamientos para la construcción (desarrollo) de aplicaciones (formatos de variables, nombres de programas, etc.), sin embargo, desarrollos significativos están a cargo de proveedores externos. La metodología de desarrollo de aplicaciones es la definida por el proveedor del servicio.	No existen procedimientos definidos para la selección de proveedores de servicios de desarrollo de aplicaciones. Además, no existe control que aseguren la aplicación de una Metodología formal para desarrollo y mantenimiento de aplicaciones por parte de los proveedores	Medio	Establecer procedimientos para definir y seleccionar proveedores de aplicaciones con base a un perfil claramente establecido y en función de las necesidades de la Empresa. Además, será necesario establecer controles relacionados con: Formulario de solicitud de requerimientos / proyectos. Establecer controles de ejecución y cumplimiento de contratos con proveedores de estos servicios. Solicitar la aplicación y cumplimientos de una metodología forma de desarrollo de sistemas.	Media
	No existen manuales técnicos de las aplicaciones, ya que el mantenimiento de las mismas son realizadas por los proveedores.	Los manuales técnicos de las aplicaciones no se encuentran actualizados.	Medio	Solicitar a los proveedores del servicio la actualización de la información de los manuales técnicos y documentación de los sistemas, con un adecuado nivel de detalle, de forma que sirvan como referencia para futuras modificaciones en los mismos	Media

Comisariato de la Policía Nacional.

Proyecto: Auditoría de Informática
Evaluación de la Situación Actual de los Servicios de Tecnología de Información Requerimiento:
Desarrollo, Operación y Mantenimiento de Aplicaciones
Objetivo de Control COBIT: Desarrollo y Mantenimiento de Procedimientos relacionados con Tecnología de Información /AI4
Administración de Operaciones /DS13
Procedimiento: Evaluar los procedimientos de operación.
Revisar las bitácoras de operación.
Revisar los procedimientos y revisar las bitácoras de ejecución de los procesos batch.

Trabajo realizado	Resultados obtenidos	Debilidades Identificadas	Nivel de riesgo	Recomendaciones	Prioridad
Revisar los lineamientos para la ejecución de procesos batch. Revisar la bitácora para control de procesos.	• Existe una rutina de ejecución de procesos en batch, la cual es ejecutada diariamente, sin embargo este proceso no se encuentra formalmente documentado. • Los procesos batch ejecutados son principalmente réplicas de las distintas bases de datos de Lotus Note. • Adicionalmente, por requerimiento de los usuarios se realizan réplicas de bases manualmente. • Los procesos batch dejan como evidencia un log histórico el cuál no es revisado periódicamente. • En el caso de excepciones, reportadas en los procesos batch cualquier persona del departamento GTS procede a solucionar a través de réplicas manuales.	No existe un procedimiento formalmente documentado sobre la ejecución y control de los procesos batch de la compañía.	Bajo	Elaborar un manual de procedimientos en el cual se detalle las responsabilidades y actividades a realizarse para ejecutar los procesos batch. Entre otras cosas, el procedimiento debería considerar: responsables, horarios, rutinas a ser ejecutadas, posibles cursos de acción en casos de problemas, etc.	Baja

Comisariato de la Policía en Masaya.

Proyecto: Auditoría de Sistemas
- Evaluación de la Situación Actual de los Servicios de Tecnología de Información Requerimiento:
Desarrollo, Operación y Mantenimiento de Aplicaciones
Objetivo de Control COBIT: Administración de la Información /DS11.
Procedimiento: Revisar los procedimientos vigentes para back up de información.
(Tipo de información, periodicidad, lugar de almacenamiento y pruebas periódicas de los respaldos).

Trabajo realizado	Resultados obtenidos	Debilidades Identificadas	Nivel de riesgo	Recomendaciones	Prioridad
Revisar los lineamientos para la obtención de respaldos.	Existe una rutina de generación de los respaldos de la información, ejecutada diariamente, sin embargo este procedimiento no está formalmente documentado. Existen respaldos diarios y mensuales. Se realizan respaldos diariamente la información del correo electrónico, servidores de archivos y base de datos de clientes. Los respaldos son completos (full) con reutilización de las cintas. Las cintas utilizadas son DLT 40/80 GB. Estas cintas pueden ser reutilizadas hasta 24 veces. Los respaldos diarios son realizados por los administradores de red.	No poseen un procedimiento formalmente documentado para el proceso de obtención de respaldos de la información. Es un proceso definido informalmente.	Medio Alto	Elaborar un manual de procedimientos en el cual se detalle el proceso de obtención de respaldos de la información, incluyendo: servidores, tipo de información, frecuencia, responsables, bitácora de novedades, etc. Establecer, difundir y hacer cumplir normas de trabajo a los usuarios que generan o procesan información sensitiva en utilitarios de oficina, como por ejemplo: - Asignar espacios definidos para cada usuario en los discos de los servidores. - Aplicar normas que obliguen a los usuarios a mantener y efectuar copias periódicas de archivos en el servidor.	

Trabajo realizado	Resultados obtenidos	Debilidades Identificadas	Nivel de riesgo	Recomendaciones	Prioridad
Revisar las actividades que realiza como medidas de respaldo de los servidores y las comunicaciones	Los procedimientos para recuperar un servidor, en caso de ocurrir una falla, no se encuentran formalmente documentados. Los servidores principales cuentan con arreglos de discos (storage arrays) y con raid 5 – tolerancia a fallas. Adicionalmente, los equipos poseen un software de monitoreo de errores en los dispositivos físicos (disco duro, tarjetas, main board, ventiladores, etc.), el cual indica constantemente los errores en los servidores	No poseen procedimientos formalmente definidos para recuperación y respaldo de servidores y comunicaciones.	Medio	Definir y documentar los requerimientos de telecomunicaciones necesarios para soportar el funcionamiento de las aplicaciones y servicios críticos estableciendo medios de comunicación alternativos (backups).	Media

Tabla 2-2

Comisariato de la Policía Nacional de Masaya.

Proyecto: Auditoría Informática

- Evaluación de la Situación Actual de los Servicios de Tecnología de Información PLATAFORMAS Y COMUNICACIONES

Requerimiento: Plataforma Tecnológica, Redes y Comunicaciones

Objetivo de Control COBIT: Administración de Desempeño y Capacidad / DS3

Procedimiento: Revisión de los procedimientos de medición del rendimiento

. Análisis de los informes de rendimiento disponibles.

Trabajo realizado	Resultado obtenido	Debilidades identificas	Nivel de riesgo	Recomendación	prioridad
Entrevista con el área de mantenimiento para relevar los procedimientos de monitoreo y rendimiento del Tráfico de la Red.	No se realizan reportes de rendimiento ni análisis del tráfico de la red. El monitoreo de la red WAN lo realiza la oficina central de Sao Paulo. Sobre la red local se realiza análisis a través de una herramienta de 3COM limitada. El control y monitoreo se efectúa a la red de acuerdo a parámetros establecidos por la organización global.	No se ha desarrollado un Plan de Administración de Capacidad de Recursos. Procedimientos para análisis de tráfico en la red y generación de reportes de rendimiento no han sido definidos.	Medio	Desarrollar un Plan de Administración de Capacidad de Recursos, en donde se establezca un proceso de revisión del desempeño y capacidad del hardware, redes y comunicaciones con el fin de asegurar que siempre existe una capacidad justificable económicamente para procesar las cargas de trabajo y proporcionar un desempeño acorde a las necesidades del negocio. El plan de capacidad deberá cubrir escenarios múltiples y procedimientos formales para el monitoreo y análisis de tráfico en la red.	Media

Comisariato de la policía de Masaya.

Proyecto: Auditoría Informática
- Evaluación de la Situación Actual de los Servicios de Tecnología de Información Requerimiento:
Plataforma Tecnológica, Redes y Comunicaciones

Objetivo de Control COBIT: Administración de Desempeño y Capacidad / DS3

Procedimiento: Revisión de los procedimientos relativos al monitoreo de la red. Análisis de la bitácora de problemas.
Análisis de los mecanismos de comunicación y acceso a los datos de la red desde el punto de vista de disponibilidad.

Trabajo realizado	Resultados obtenidos	Debilidades Identificadas	Nivel de riesgo	Recomendación	Prioridad
	No se dispone localmente de herramientas para monitoreo. No se cuenta con procedimientos formales para el control de eventos en la red.	No se emiten reportes periódicos del monitoreo a la red y comunicaciones. Además, no se utiliza software para el monitoreo de las red y comunicaciones.	Alto	Implementar procedimientos de Monitoreo y Reporte de Eventos de la Red y las Comunicaciones. Asimismo, las excepciones deberán ser reportadas y registradas en una bitácora de problemas de manera oportuna y completa. Los reportes deberán incluir la capacidad de pronóstico para permitir que los problemas sean solucionados antes que afecten en forma perceptible el desempeño del sistema de información. Nos permitimos sugerir se utilicen las siguientes herramientas. • Monitor del Sistema de Window 8 • HP Open View, herramienta compatible con Manager, que posee entre otras las siguientes utilidades: • Monitoreo de Comunicaciones • Monitoreo de Infraestructura de Internet. • Administración de Redes LAN. • Administración de recursos y rendimiento.	Alta

5.18 Informe Final de la Auditoria de Tecnología de la Información.

COMISARIATO DE LA POLICIA NACIONAL MASAYA
Managua, 29 de diciembre del 2014.
Antonio Franco
JEFE DEL ÁREA DE INFORMÁTICA

De nuestra consideración:
Tenemos el agrado de dirigirnos a Ud. a efectos de elevar a vuestra consideración el alcance del trabajo de Auditoría del Área de Informática practicada en el periodo de enero a diciembre del 2014, sobre la base del análisis y procedimientos detallados de todas las informaciones recopiladas y emitidos en el presente informe, que a nuestro criterio es razonable.

Síntesis de la revisión realizada, clasificado en las siguientes secciones:
1. En su Seguridad
2. En el área Física
3. En Redes
El contenido del informe ha sido dividido de la siguiente forma a efectos de facilitar su análisis.
a. Situación. Describe brevemente las debilidades resultantes de nuestro análisis.
b. Efectos y/o implicancias probables. Enuncian los posibles riesgos a que se encuentran expuestos las operaciones realizadas.
c. Índice de importancia establecida. Indica con una calificación del 0 al 3 el grado crítico del problema y la oportunidad en que se deben tomar las acciones correctivas del caso.
0 = Alto (acciones correctivas inmediatas)
1 = Alto (acciones preventivas inmediatas)
2 = Medio (acciones diferidas correctivas)
3 = Bajo (acciones diferidas preventivas)

Según el análisis realizado hemos encontrado falencias en que no existe un Comité y plan informático; falencias en la seguridad física y lógica; no existe auditoria de sistemas; falta de respaldo a las operaciones; accesos de los usuarios.

El detalle de las deficiencias encontradas, como así también las sugerencias de solución se encuentran especificadas en el Anexo adjunto. La aprobación y puesta en práctica de estas sugerencias ayudarán a la empresa a brindar un servicio más eficiente.

Agradecemos la colaboración prestada durante nuestra visita por todo el personal del CPN Masaya quedamos a vuestra disposición para cualquier aclaración y/o ampliación de la presente que estime necesaria.

Atentamente,

_____
Msc. Francisco Pérez
Auditor Interno
CPN Managua

A. Organización y Administración del Área

A.1. Comité y Plan Informático

a. Situación

Con respecto al relevamiento efectuado, hemos notado lo siguiente:

• No existe un Comité de Informática o al menos no se encuentra formalmente establecido.

• No existe ninguna metodología de planificación, concepción y/o seguimiento de proyectos.

b. Efectos y/o implicancias probables

• Posibilidad de que las soluciones que se implementen para resolver problemas operativos sean parciales, tanto en Hardware como en Software.

c. Índice de importancia establecida 1 (uno)

d. Sugerencias

• Establecer un Comité de Informática integrado por representantes de las áreas funcionales claves (Gerencia Administrativa, responsables de las Áreas Operativas, responsables de Informática y el responsable Contable).

• Trazar los lineamientos de dirección del Área de Informática.

• Implementar normas y/o procedimientos que aseguren la eficaz administración de los recursos informáticos, y permitan el crecimiento coherente del área conforme a la implementación de las soluciones que se desarrollen y/o se requieran de terceros.

• Efectos y/o implicancias probables

• La escasez de personal debidamente capacitado, aumenta el nivel de riesgo de errores al disminuir la posibilidad de los controles internos en el procesamiento de la información; y limita la cantidad de soluciones que pueden implementarse en tiempo y forma oportuna a los efectos de satisfacer los requerimientos de las áreas funcionales.

B. Seguridad Física Y Lógica

B.1. Entorno General

a. Situación Durante nuestra revisión, hemos observado lo siguiente:

• No existe una vigilancia estricta del Área de Informática por personal de seguridad dedicado a este sector.

• No existe detectores, ni extintores automáticos.

• Existe material altamente inflamable.

• Carencia de un estudio de vulnerabilidad, frente a las riesgos físicos o no físicos, incluyendo el riesgo Informático.

• No existe un puesto o cargo específico para la función de seguridad Informática.

b. Efectos y/o implicancias probables

• Probable difusión de datos confidenciales.

• Alta facilidad para cambios involuntarios o intencionales de datos, debido a la falta de controles internos.

• Debido a la debilidad del servicio de mantenimiento del equipo central, la continuidad de las actividades informáticas podrían verse seriamente afectadas ante eventuales roturas y/o desperfectos de los sistemas.

c. Índice de importancia establecida 0 (cero)

d. Sugerencias

A los efectos de minimizar los riesgos descriptos, se sugiere:

• Establecer guardia de seguridad, durante horarios no habilitados para el ingreso al Área de Informática.

• Colocar detectores y extintores de incendios automáticos en los lugares necesarios.

• Remover del Centro de Cómputos los materiales inflamables.

• Determinar orgánicamente la función de seguridad.

• Realizar periódicamente un estudio de vulnerabilidad, documentando efectivamente el mismo, a los efectos de implementar las acciones correctivas sobre los puntos débiles que se detecten.

B.2. Auditoría de Sistema

a. Situación

• Hemos observado que la Municipalidad no cuenta con auditoría Informática , ni con políticas formales que establezcan responsables, frecuencias y metodología a seguir para efectuar revisiones de los archivos de auditoría.

• Cabe destacar que el sistema integrado posee un archivo que pudiera servir de auditoria Informática, el cual no es habilitado por falta de espacio en el disco duro.

b. Efectos y/o implicancias probables

• Posibilidad de que adulteraciones voluntarias o involuntarias sean realizadas a los elementos componentes del procesamiento de datos (programas, archivos de datos,

definiciones de seguridad de acceso, etc) o bien accesos a datos confidenciales por personas no autorizadas que no sean detectadas oportunamente.

c. Índice de importancia establecida

d. Sugerencias

• Establecer normas y procedimientos en los que se fijen responsables, periodicidad y metodología de control de todos los archivos de auditoría que pudieran existir como asimismo, de todos los elementos componentes de los sistemas de aplicación.

B.3. Operaciones de Respaldo

a. Situación

Durante nuestra revisión hemos observado que:

• Existe una rutina de trabajo de tomar una copia de respaldo de datos en Disckett, que se encuentra en el recinto del centro de cómputos, en poder del auxiliar de informática.

• Si bien existen la copia de seguridad, no se poseen normas y/o procedimientos que exijan la prueba sistemática de las mismas a efectos de establecer los mínimos niveles de confiabilidad.

b. Efectos y/o implicancias probables

• La Cooperativa está expuesta a la perdida de información por no poseer un chequeo sistemático periódico de los back-up's, y que los mismas se exponen a riesgo por encontrarse en poder del auxiliar de informática.

c. Índice de importancia establecida

d. Sugerencias

Minimizar los efectos, será posible a través de:

• Desarrollar normas y procedimientos generales que permitan la toma de respaldo necesarios, utilitario a utilizar.

• Realizar 3 copias de respaldos de datos en Zip de las cuales, una se encuentre en el recinto del área de informática, otra en la sucursal más cercana y la última en poder del Jefe de área.

• Implementar pruebas sistemáticas semanales de las copias y distribución de las mismas.

B.4. Acceso a usuarios

a. Situación

De acuerdo a lo relevado hemos constatado que:

• Existen niveles de acceso permitidos, los cuales son establecidos conforme a la función que cumple cada uno de los usuarios.

• Los usuarios definidos al rotar o retirarse del local no son borrados de los perfiles de acceso.

• Las terminales en uso y dado un cierto tipo de inactividad no salen del sistema.

• El sistema informático no solicita al usuario, el cambio del Password en forma mensual.

b. Efectos y/o implicancia probables

• Existe la imposibilidad de establecer responsabilidades dado que esta se encuentra dividida entre el área de sistema y los usuarios finales.

• La falta de seguridad en la utilización de los Password, podrían ocasionar fraudes por terceros.

c. Índice de importancia establecida (2)

d. Sugerencia

• Implementar algún software de seguridad y auditoria existente en el mercado o desarrollar uno propio.

• Establecer una metodología que permita ejercer un control efectivo sobre el uso o modificación de los programas o archivos por el personal autorizado.

B.5. Plan de Contingencias

a. Situación: En el transcurso de nuestro trabajo hemos observado lo siguiente:

• Ausencia de un Plan de Contingencia debidamente formalizado en el Área de Informática.

• No existen normas y procedimientos que indiquen las tareas manuales e informáticas que son necesarias para realizar y recuperar la capacidad de procesamiento ante una eventual contingencia (desperfectos de equipos, incendios, cortes de energía con más de una hora), y que determinen los niveles de participación y responsabilidades del área de sistemas y de los usuarios.

• No existen acuerdos formalizados de Centro de Cómputos paralelos con otras empresas o proveedores que permitan la restauración inmediata de los servicios informáticos de la Cooperativa en tiempo oportuno, en caso de contingencia.

b. Efectos y/o implicancia probable

• Pérdida de información vital.

• Pérdida de la capacidad de procesamiento.

c. Índice de Importancia relativa

d. Sugerencias

• Establecer un plan de contingencia escrito, en donde se establezcan los procedimientos manuales e informáticos para restablecer la operatoria normal y establecer
Los responsables de cada sistema.

• Efectuar pruebas simuladas en forma periódica, a efectos de monitorear el desempeño de los funcionarios responsables ante eventuales desastres.

• Establecer convenios bilaterales con empresas o proveedores a los efectos de asegurar los equipos necesarios para sustentar la continuidad del procesamiento.

C. Desarrollo y mantenimiento de los sistemas de aplicaciones

C.1. Entorno de Desarrollo y mantenimiento de las aplicaciones

a. Situación

• No existe documentaciones técnicas del sistema integrado y tampoco no existe un control o registro formal de las modificaciones efectuadas.

• No se cuenta con un Software que permita la seguridad de las librerías de los programas y la restricción y/o control del acceso de los mismos.

• Las modificaciones a los programas son solicitadas generalmente sin notas internas, en donde se describen los cambios o modificaciones que se requieren.

Para reducir el impacto sobre los resultados de los efectos y consecuencias probables sugerimos:

• Elaborar toda la documentación técnica correspondiente a los sistemas implementados y establecer normas y procedimientos para los desarrollos y su actualización.

• Evaluar e implementar un software que permita mantener el resguardo de acceso de los archivos de programas y aún de los programadores.

• Implementar y conservar todas las documentaciones de prueba de los sistemas, como así también las modificaciones y aprobaciones de programas realizadas por los usuarios

VI. CONCLUSIONES.

Al finalizar el desarrollo de este trabajo investigación de la evaluación técnica e informática de los sistemas tecnológicos de información, dela Comisariato de la Policía Nacional, se han cumplido con los objetivos propuestos en el presente trabajo, por lo tanto se exponen a continuación las siguientes conclusiones y recomendaciones en torno a la realización del proyecto.

- Para el desarrollo de una Auditoría Informática de los Sistemas de Información es de principal importancia contar con la guía de un marco de referencia. Para este proyecto se ha escogido el modelo COBIT desarrollado por ISACA, el cual el cual a través de sus 4 dominios ofrece una serie de objetivos de control que permiten evaluar eficientemente el ambiente de control de una entidad, garantizando que TI está alineada con el negocio y que los riesgos de TI se administren apropiadamente.
- Al alinear la Normativa de Tecnologías de la Información y los objetivos de control propuestos por COBIT se logró identificar y valorar los riesgos dentro de la entidad para tomar las medidas pertinentes y minimizar la materialización de los riesgos identificados.
- Durante el análisis y evaluación del ambiente de control en la entidad aplicando los dominios propuestos por COBIT se logró identificar debilidades obteniendo observaciones y recomendaciones para ser emitidas en el informe final, para llevar a cabo el proceso de la Auditoría es de suma importancia contar con el compromiso y apertura a la Auditoría Informática de los sistemas de información; de los principales involucrados como son las Autoridades superiores de la Cooperativa, el personal del departamento de sistemas y el Departamento de Auditoría Interna.
- La Auditoría de TI propone mejoras a los controles existentes en la misma, pues sabiendo que si los controles facilitan la rendición de cuentas mediante la evidencia; al mejorar los controles que están fallando se logrará mitigar los riesgos. La Administración debe identificarse y conocer plenamente los controles.
- De acuerdo con lo planteado y el proyecto realizado es responsabilidad de la entidad aplicar y poner en marcha las recomendaciones emitidas de la Auditoría Informática, llevando a cabo esto de acuerdo a su capacidad y crecimiento.
- Luego de la revisión se analizó el nivel de madurez en que actualmente se encuentra la empresa según los riesgos y fallas encontradas y se determina el nivel al que se puede ascender si se cumplen con las recomendaciones planteadas.

VII. ANEXOS

Anexo 1: Detalle del Personal.

Comisariato de la Policía Nacional

AUDITORIA INTERNA

PLAN DE TRABAJO: ENERO - DICIEMBRE 2014

ENERO A DICIEMBRE DE 2014

Tabla. No. 1

No.	Nombre y Apellidos	Cargo	Horas Disponible
1	AUDITOR INTERNO - Lic. Francisco Pérez	Auditor Interno	1760
2	Auditor Supervisor Area Contable- Lic. Margarita Calero	Supervisor	1760
3	Auditor Superior Area de Sistemas- Ing. Marvin Saravia	Supervisor	1760
4	Ingeniero en Informatica - Ing. Miguel Gomez	Encargado	1760
5	Técnico en Desarrollo - Edwin Lopez	Asistente	1760
6	Técnico en Infraestructura- Mariana Ortiz	Asistente	1760
7	Técnico en Mantenimiento - Benjamin Martinez	Asistente	1760
8	Secretaria Ejecutiva - Camila Torrez	Asistente	1760
TOTAL HORAS HOMBRES DISPONIBLES			**14,080**

Fuente: Archivo de Expediente de Auditoria CPN Managua.

4.6 Capacidad Instalada de la unidad de Auditoria Interna. (Anexo 2)

Comisarito de la Policia Nacional

Capacidad Instalada de la Unidad de Auditoria Interna

Tabla No. 2

PARA EL PERIODO DE ENERO A DICIEMBRE DE 2014

EMPRESA: CPN Masaya **PLAN DE TRABAJO: ENERO - DICIEMBRE 2014**

					MENOS					
Nº	NOMBRE COMPLETO	CARGO	PROFESIÓN	DIAS ANUALES	SABADOS Y DOMINGOS	VACACIONES	FERIADOS	CAPACITACIONES	DIAS DISPONIBLES	HORAS DISPONIBLES
1	Francisco Pérez	Auditor Interno	Lic. Contaduría Pública	365	96	30	9	10	220	1760
2	Margarita Calero	Supervisor	Lic. Contaduría Pública	365	96	30	9	10	220	1760
3	Marvin Sarvia	Supervisor	Ing. Informatico	365	96	30	9	10	220	1760
4	Miguel Gomez	Encargado	Ing. Sistema	365	96	30	9	10	220	1760
5	Edwin Lopez	Asistente	Ing. Sistema	365	96	30	9	10	220	1760
6	Mariana Ortiz	Asistente	Ing. Informatico	365	96	30	9	10	220	1760
7	Benjamin Martinez	Asistente	Ing. Informatico	365	96	30	9	10	220	1760
8	Camila Torrez	Asistente	Secretaria Ejecutiva	365	96	30	9	10	220	1760
				Total Horas Disponibles						**14080**

Elaborado Por: _____ **Autorizado por:_____**

Auditor Interno **Auditor Interno**

Fuente: Archivo de Expediente de Auditoria CPN Managua.

Anexo 3

Comisariato Policia Nacional
PLAN DE TRABAJO : ENERO A DICIEMBRE DE 2014
AUDITORIA INTERNA

Aplicarse a: Comisariato Policia Nacional Masaya

PLAN DE TRABAJO ENERO A DICIEMBRE DE 2014

Nº	Actividad	Area sujeta a control	Objetivos Generales de la Actividad	Personal Designado	Fechas Estimadas: Inicio	Fechas Estimadas: Finalización	Horas Hombre	Relación o Coordinación
1	Ejercer el control previo de los procesos informaticos de la empresa.	Empresa en general	Conocer la situacion informatica real desarrollado en la empresa.	Auditor Interno Auditor Supervisor	02/01/2014	01/03/2014	1,250	Contabilidad Gerencia General Almacen, Facturacion, Informatica
			Verificar el cumplimiento de los procedimientos de control interno establecidos para la realización de la actividad, desde su inicio hasta su finalización					
			Evaluación de sistemas, procedimientos y equipos de cómputo.					
			Verificar que los activos, estén debidamente controlados y salvaguardados contra pérdida y mal uso.					
2	Evaluar el control interno informatico implementado en la empresa	Area Informatica	Evaluar la efectividad y eficacia del diseño y operación del control interno informatico implementado en la empresa	Auditor Interno; Supervisor, Auditor Encargado, Asistente	01/03/2014	30/05/2014	1,300	Contabilidad Gerencia General Almacen, Facturacion, Informatica
			Evaluar los resultados de los programas operativos que realice el área de Sistemas para conocer eficiencia y efectividad con que se han utilizado los recursos.					
3	Implementación de las entrevistas y pruebas de confirmaciones con el fin de recopilar hallazgos para desarrollar la auditoria	Administracion y Area informatica	Elaboración de cuestionarios, encuestas, matrices y herramientas que ayuden al levantamiento de la información para el debido desarrollo de las auditorías.	Auditor Interno; Supervisor, Auditor Encargado, Asistente	01/06/2014	30/09/2014	6,030	Contabilidad Gerencia General Almacen, Facturacion, Informatica
			Constatar que el área de sistemas se rija por los procedimientos más adecuados para garantizar el adecuado funcionamiento de la red de trabajo.					
			Implementación de los planes de trabajo llevando un control de las actividades a realizar en tiempos estimados reales.					
4	Realización de Informe Final de acuerdo a las hallazgos encontrados	Empresa en general	1. Evaluar la problemática del área de Sistemas a través de un pre-análisis de la situación del área, para la determinación de las principales necesidades de ésta.	Auditor Interno; Auditor Encargado]Supervisor	01/10/2014	30/12/2014	2,600	Contabilidad Gerencia General Almacen, Facturacion, Informatica
			2. Comunicar los resultados y recomendaciones que resulten de sus evaluaciones, mediante los informes de auditoría.					
			3. Comprobar que el área de Sistemas ha tomado las medidas correctivas de los informes de la Auditoría Interna así como de las omisiones que al respecto se verifiquen en el seguimiento de informes.					
			4. Evaluación de los controles de seguridades lógicas y físicas que garanticen la integridad, confidencialidad y disponibilidad de los datos de esta institución.					
				Sub-Total Horas Hombres			**11,180**	

Comisariato Policia Nacional
PLAN DE TRABAJO : ENERO A DICIEMBRE DE 2014
AUDITORIA INTERNA

Aplicarse a: Comisariato Policia Nacional Masaya

PLAN DE TRABAJO ENERO A DICIEMBRE DE 2014

Nº	Actividad	Area sujeta a control	Objetivos Generales de la Actividad	Personal Designado	Fechas Estimadas: Inicio	Fechas Estimadas: Finalización	Horas Hombre	Relación o Coordinación
4	Capacitación 5%	Fortalecer el nivel y calidad de los funcionarios de la Auditoria Interna y por ende la calidad de los trabajos					**500**	
5	Actividades de arrastre, con un avance del 30%	Concluir en el primer trimestre del año 2014 las actvidades pendientes del 2013, cuyo avance alcanzo al 31 de diciembre de 2013 el 30%					**800**	
6	Actividades extraplan	Ejecutar las actividades extraplan solicitadas					**800**	
7	Actividades Administrativas 5%	Obtener el soporte logistico de la Administracion					**800**	
					Sub - Total Horas Hombre		**2,900**	
					Gran Total Horas Hombre		**14,080**	

Elaborado Por: _____
AUDITOR INTERNO
EL AUDITOR

Autorizado por:_____
EL AUDITOR INTERNO

Fuente: Archivo de Expediente de Auditoria CPN Managua.

Anexo 4: Presupuesto de tiempo en horas

Presupuesto de Tiempo en horas por Persona
Inicio de la Auditoría con presentación de credencial

Actividades	Auditor Interno	Auditori Supervisor 1	Auditor Supervisor 2	Auditor Encagado	Asistente	Asistente	Asistente	Asistente	Total
Fase I - Planeación de la Auditoría / Revisión	**750**	**500**	**500**	**300**	**200**	**200**	**200**	**200**	**2850**
Notificación inicial de la revisión / auditoría	**200**	**100**	**100**	**80**	50	50	50	50	680
Identificación de las leyes, normas, regulaciones y otros aplicables	150	150	150	80	50	50	50	50	730
Elaboración del memorandum de planeación	300	150	150	90	50	50	50	50	890
Elaboración del programa de auditoría / revisión	100	100	100	50	50	50	50	50	550
Fase II - Ejecución del trabajo de campo	**0**	**800**	**800**	**1000**	**1410**	**1410**	**1410**	**1410**	**8240**
1. Solicitud de requerimientos iniciales		**120**	**120**	**120**	150	150	150	150	960
2. Análisis de la documentacion obtenida		**120**	**120**	**240**	150	150	150	150	1080
3. Realizar de pruebas iniciales o procedimientos de revisión definidos		**100**	**100**	**150**	360	360	360	360	1790
4. Verificar las políticas y procedimientos aplicables a la revisión		**120**	**120**	**100**	350	350	350	350	1740
5. Realización de las pruenas finales de auditoría y revisión		**120**	**120**	**200**	200	200	200	200	1240
6. Elaboración de hallazgos de la revisión		**120**	**120**	**100**	100	100	100	100	740
7.- Discución con los auditados de los hallazgos de la revisión		**100**	**100**	**90**	100	100	100	100	690
Fase II - Conclusión de la auditoría / revisión	**1010**	**460**	**460**	**460**	**150**	**150**	**150**	**150**	**2990**
1. Análisis de la respuesta de los auditados a los hallazgos de la revisión	150	120	120	120					510
2. Emisión del borrador del informe	230	180	180	180	150	150	150	150	1370
3. Revisión del borrador del informe	280	70	70	70					490
4. Emisión del informe en definitivo	350	90	90	90					620
Totales	**1760**	**1760**	**1760**	**1760**	**1760**	**1760**	**1760**	**1760**	**14080**

Presupuesto de Costo de la Auditoria.

Fuente: Archivo de Expediente de Auditoria CPN Managua.

Anexo 5

UNIDAD DE AUDITORÍA INTERNA
COMISARITO DE LAPOLICIA NACIONAL
PRESUPUESTO DE COSTOS DE AUDITORÍA
(EXPRESADO EN CÓRDOBAS)

Area y/o Unidad a Auditar: Area Informatica CPN masaya **Clase de auditoría/ revisión: Auditoria Informatica**

Fecha de Inicio: 02/01/2014 **Fecha de Conclusión: 31/12/2014**

Cargo	Valor H/H	Días	Horas/Hombre	Salario ANUAL	Alimentación	Transporte	Hospedaje	Total
Auditor Interno	90.00	220.0	1760	158,400.00				158,400.00
Supervisor	80.00	220	1760	140,800.00				140,800.00
Supervisor	80.00	220	1760	140,800.00				140,800.00
Encargado	60.00	220	1760	105,600.00				105,600.00
Asistente	50.00	220	1760	88,000.00				88,000.00
Asistente	50.00	220	1760	88,000.00				88,000.00
Asistente	50.00	220	1760	88,000.00				88,000.00
Asistente	50.00	220	1760	88,000.00				88,000.00
Total			14080	**897,600.00**	-	-	-	**897,600.00**

Gastos Estimados	**COSTO TOTAL**
Salarios	897,600.00
Prestaciones Sociales (6)	323,136.00
Viáticos	
Papelería y útiles de oficina (7)	17,952.00
Total	**1238,688.00**

1) Valor horas-hombre. Salario mensual entre 240 horas laborables al mes.
2) Tiempo Estimado
4) Salario es igual a multiplicar el valor hora hombre por el número de horas (Salario= 1*3
5) En el viático se multiplica el número de días por el valor del viático (si aplica)
6) Prestaciones Sociales el 36% de Salario (al total casilla (4) por 36%
7) Papelería y útiles de oficina el 2% del total de la suma del salario del Encargado y Asistente de trabajar solo el Auditor interno se aplica dicho porcentaje a su salario casilla (4)

Fuente: Archivo de Expediente de Auditoria CPN Managua.

Elaborado
Lic. Francisco Perez
Auditora Interna

Anexo 6

COMISARIATO DE LA POLICIA NACIONAL
UNIDAD DE AUDITORÍA INTERNA

Auditoría /Revisión: AUDITORIA DE TECNOLOGIA DE LA INFORMACION

Fechas estimadas de Auditoria / Revisión:

Proceso de la auditoría	Fecha de ejecución		Semanas	Días	Horas	%
Planeación de la auditoría / revisi	02/01/2014	01/03/2014	12	84	1250	8.88
Ejecución y Finalización de Trab.	01/03/2014	30/09/2014	28	196	10230	72.66
Comunicación de Resultado	01/10/2014	31/12/2014	12	84	2600	18.47
	Total		**52**	**364**	**14080**	100

14080

Horas Hombres Utilizadas por el Equipo de Auditoría

Personal de Audi	Días	Horas	Planeación	Ejecución	Emision		Total
Auditor Interno	220.00	1760	750		1010		**1760**
Supervisor	220.00	1760	500	800	460		**1760**
Supervisor	220	1760	500	800	460		**1760**
Encargado	220	1760	300	1000	460		**1760**
Asistente	220	1760	200	1410	150		**1760**
Asistente	220	1760	200	1410	150		**1760**
Asistente	220	1760	200	1410	150		**1760**
Asistente	220	1760	200	1410	150		**1760**
Total	1760.00	**14080**	2850	8240	2990		**14080**

Fuente: Archivo de Expediente de Auditoria CPN Managua.

Anexo 7: Control Interno Informático

El Control Interno en las empresas tiene como finalidad ayudar en la evaluación de la eficacia y eficiencia de la gestión administrativa.

Objetivos del control interno informático:

- Establecer como prioridad la seguridad y protección de la información del sistema computacional y de los recursos informáticos de la empresa.
- Promover la confiabilidad, oportunidad y veracidad de la captación de datos, su procesamiento en el sistema y la emisión de informes en la empresa.
- Implementar los métodos, técnicas y procedimientos necesarios para coadyuvar al eficiente desarrollo de las funciones, actividades y tareas de los servicios computacionales, para satisfacer los requerimientos de sistemas en la empresa.
- Instaurar y hacer cumplir las normas, políticas y procedimientos que regulen las actividades de sistematización de la empresa.
- Establecer las acciones necesarias para el adecuado diseño e implementación de sistemas computarizados, a fin de que permitan proporcionar eficientemente los servicios de procesamiento de información en la empresa.

Elementos fundamentales del control interno informático

- Controles internos sobre la organización del área de informática
- Controles internos sobre el análisis, desarrollo e implementación de sistemas
- Controles internos sobre operación del sistema
- Controles internos sobre los procedimientos de entrada de datos, el procesamiento de información y la emisión de resultados.
- Controles internos sobre la seguridad del área de sistemas.

Cuadro del control interno en el área de Informática

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

➢ Implementar y mantener la seguridad en la operación ➢ Mantener la confiabilidad, oportunidad, veracidad y suficiencia en el procesamiento de la información de la institución
Controles internos sobre los procedimientos de entrada de datos, el procesamiento de información y la emisión de resultados. ➢ Verificar la existencia y funcionamiento de los procedimientos de captura de datos ➢ Comprobar que todos los datos sean debidamente procesados ➢ Verificar la confiabilidad, veracidad y exactitud del procesamiento de datos. ➢ Comprobar la oportunidad, confiabilidad y veracidad en la emisión de los resultados del procesamiento de información.
Controles internos sobre la seguridad del área de sistemas ➢ Controles para prevenir y evitar las amenazas, riesgos y contingencias que inciden en las áreas de sistematización. ➢ Controles sobre la seguridad física del área de sistemas ➢ Controles sobre la seguridad lógica de los sistemas. ➢ Controles sobre la seguridad de las bases de datos ➢ Controles sobre la operación de los sistemas computacionales ➢ Controles sobre seguridad del personal de informática ➢ Controles sobre la seguridad de la telecomunicación de datos ➢ Controles sobre la seguridad de redes y sistemas multiusuarios

PERFILES DE PUESTOS

Este elemento del control interno informático ayuda a identificar y establecer los requisitos, habilidades, experiencia y conocimientos específicos que necesita tener el personal que ocupa un puesto en el área de sistemas. Se debe de considerar dentro del perfil de puestos cada una de las características que deben poseer quienes ocupan los puestos que integran la estructura de organización del centro informático de la empresa. Aunque la existencia de este documento es fundamental para el control interno informático a veces quienes dirigen estas áreas de sistemas dejan de utilizarlo debido a que no es fácil definir perfiles de puestos en un centro de cómputo, porque desconocen su utilidad o simplemente porque ignoran la importancia de considerar en su diseño los siguientes aspectos:

- La forma de operación establecida para cada puesto, de acuerdo con los sistemas de cómputo de la empresa.
- Las necesidades de procesamiento de datos, desde la captura hasta la emisión de resultados.
- La configuración de los equipos, instalaciones y componentes de la rea de sistemas, incluyendo su arquitectura y la forma de administración de los mismos.
- La manera cómo influye esta delineación en el uso de los recursos informáticos tanto de hardware y software como de los recursos técnicos de comunicación y del propio factor humano informático especializado.

Con el perfil de puestos se pretende estandarizar hasta donde es posible, los requisitos mínimos que se deben contemplar para cada uno de los puestos del centro informático.
Es trascendental destacar la importancia del uso del perfil de puestos para la selección adecuada del personal que ocupara los puestos dentro del área de sistemas, debido a que en este documento se establecerán en forma precisa y correcta las características,

conocimientos y habilidades que deberán tener quienes ocupen dichos puestos. Esto será la garantía de un desarrollo eficiente y eficaz de las funciones y actividades de cada puesto.

Controles internos para la operación del sistema

Permite evaluar la adecuada operación de los sistemas, se requiere de un elemento que se encargue de vigilar y verificar la eficiencia y eficacia en la operación de dichos sistemas, su existencia ayuda a garantizar el cumplimiento de los objetivos básicos del control interno. Permite:

- Prevenir y corregir errores de operación
- Prevenir y evitar la manipulación fraudulenta de la información
- Implementar y mantener la seguridad en la operación
- Mantener la confiabilidad, oportunidad, veracidad y suficiencia en el procesamiento de la información en la institución

Controles internos para los procedimientos de entrada de datos, procesamiento de información y emisión de resultados

Son de gran ayuda por la confiabilidad que brindan en el procesamiento de información, permiten verificar que el procedimiento de entrada-proceso-salida se lleve a cabo correctamente.

- Verificar la existencia y funcionamiento de los procedimientos de captura de datos. Es evidente que se requiere un adecuado control en la entrada delos datos que han de ser procesados en cualquier sistema computacional ya que de esto depende que se obtengan buenos resultados.
- Comprobar que los datos sean debidamente procesados.
- Verificar la confiabilidad, veracidad y exactitud del procesamiento de datos
- Comprobar la suficiencia de la emisión de información.- La información debe ser adecuada a los requerimientos de la empresa para ofrecer solo la información requerida, sin dar ni más ni menos datos que los necesarios, a esto se le llama *proporcionar información suficiente.*

Controles internos para la seguridad del área de sistemas

Seguridad de los recursos informáticos, del personal, de la información, de sus programas, etc., lo cual se puede lograr a través de medidas preventivas o correctivas, o mediante el diseño de programas de prevención de contingencias para la disminución de riesgos.

Controles para prevenir y evitar amenazas, riesgos y contingencias en las aéreas de sistematización

- Control de accesos físicos del personal del área de computo
- Control de accesos al sistema, a las bases de datos, a los programas y a la información
- Uso de niveles de privilegios para acceso, de palabras clave y de control de usuarios
- Monitoreo de accesos de usuarios, información y programas de uso
- Existencia de manuales e instructivos, así como difusión y vigilancia del cumplimiento de los reglamentos del sistema
- Identificación de los riesgos y amenazas para el sistema, con el fin de adoptar las medidas preventivas necesarias
- Elaboración de planes de contingencia, simulacros y bitácoras de seguimiento

HERRAMIENTAS DE CONTROL

Las herramientas de control (software) más comunes son:

- Seguridad lógica del sistema
- Seguridad lógica complementaria al sistema (desarrollado a la medida)
- Seguridad lógica para entornos distribuidos
- Control de acceso físico. Control de presencia.
- Control de copias
- Gestión de soportes magnéticos
- Gestión y control de impresión y envío de listados por red
- Las cuentas de usuarios deben ser asignadas a un solo usuario.
- Cada usuario debe estar asociado a un perfil. Los perfiles a su vez deben estar compuestas por roles. Se deberá procurar que exista una adecuada segregación de funciones en la asignacion de perfiles y roles a los usuarios.
- Durante el inicio de la sesión el usuario y la contraseña deben de viajar encriptados a través de la red de datos.
- La longitud de las contraseñas debe de ser de por lo menos seis caracteres y su vez debe de estar compuesta por letras, números y símbolos especiales.
- Las contraseñas deben de ser ocultadas al Usuario mientras son escritas.
- En el primer inicio de sesión debe ser cambiada la contraseña por el Usuario.
- Las contraseñas deben ser cambiadas periódicamente, cada 30 o 60 días o cuando el Usuario lo requiera hacer sin límites 130 de veces. Una vez definida la política para la expiración de contraseñas, el recordatorio de cambio de contraseña debe ser automático para el Usuario.
- El acceso a los recursos tecnológicos debe estar restringidos a horarios y días específicos para cada perfil de Usuario.
- En los sistemas de información a más del Usuario y la Contraseña, podría validarse la dirección IP o el MAC Adres de la estación de trabajo.
- Dentro de las políticas de red debería establecerse que cada cierto tiempo de inactividad el equipo se bloquee a través del protector de pantalla el cual deberá estar protegido por la contraseña de inicio de sesión.

En cuanto a la Gestión de Riesgo de la Planificación y Organización se recomienda lo siguiente:

- La existencia de un cargo de Administración de Redes y Comunicaciones cuyas funciones estén claramente segregadas y diferenciadas a las del Administrador de Sistemas, Operaciones, Bases de Datos u otro cargo dentro del área de TI, de tal manera que se evite la incompatibilidad de funciones.
- Políticas y procedimientos claramente definidos respecto a la administración, operación, monitoreo, calidad, seguridad y de recuperación frente a desastres, para cada uno de los servicios de redes y comunicaciones. Esto incluye la formalización de una arquitectura de redes y comunicaciones y el diseño de los diagramas de las redes LAN y WAN.
- Políticas y procedimientos formalmente definidos para el registro, seguimiento y corrección de incidentes para garantizar que se tomen medidas de acción preventivas para disminuir su probabilidad de ocurrencia y mitigar su impacto en el futuro.
- Una política de seguridad y alta disponibilidad para garantizar que la Entidad asuma la responsabilidad de asegurar la inversión en nuevas tecnologías de hardware y software que le permitan disminuir el riesgo de ataques externos e internos contra la seguridad de sus aplicaciones, servidores y demás recursos conectados a la red de datos.
- Una participación proactiva del Administrador de Redes y Comunicaciones dentro del diseño y mantenimiento de las aplicaciones de software mediante la recomendación de controles y medidas de seguridad para garantizar la eficiencia, calidad e integridad de la información mientras es transmitida a través de la red de datos.
- De existir varias personas dentro de la función de redes y comunicaciones, deberá establecerse las funciones, responsabilidades y procesos de cada cargo y definir un orden jerárquico funcional.
- Formalizar los procesos, actividades y tareas del área o función de redes y comunicaciones; así como los estándares de cableado estructurado, hardware (equipos activos) y software a seguirse; y, los niveles de autorización y acceso a la red de datos.
- Contratos debidamente firmados entre la Entidad y sus diversos proveedores de servicios de redes y comunicaciones tercerizados, que incluyan acuerdos de confidencialidad, niveles de calidad servicio (up-time) y penalizaciones por incumplimiento.

Respecto a la Gestión de Riesgo de la Red Física es importante mencionar:

• Deben existir controles adecuados para garantizar la seguridad de los equipos principales de redes y comunicaciones ubicados en el Centro de Cómputo contra accesos no autorizados.

• El cableado estructurado deberá estar protegido por canaletas (dentro de la Oficina) y por tubería EMT (fuera de la Oficina) para garantizar que no sean manipulados, dañados o "pinchados".

• Realizar pruebas periódicas al cableado de datos mediante dispositivos de control y monitoreo para garantizar su correcto funcionamiento y calidad de transmisión.

• Disponer de acometidas de cableado estructurado de backup para ser utilizados en caso de contingencias.

• Los equipos de comunicaciones deben ser ubicados en racks cerrados con llave en ambientes seguros con condiciones ambientales adecuadas y bajo estándares de instalación, adecuadamente organizados y ubicados.

• Seleccionar en forma minuciosa al personal externo de electricidad, mantenimiento y de telefonía e implementar los controles necesarios de vigilancia y supervisión cuando estos realicen trabajos en el Entidad, tanto dentro como fuera de los horarios de oficina.

• Los Patch Panel de Enlace y especialmente el Patch Panel de Core, Switches y acometidas de cableado estructurado deberán estar etiquetados para identificar cada puerto, dispositivo y cable instalado dentro de la red de datos.

• Se deberá procurar mantener un centro de comunicaciones alterno fuera de la Oficina Matriz para casos graves de desastre, así como enlaces de transmisión de datos y de Internet de backup.

Sobre la Gestión de Riesgo de la Red Lógica se exhorta tomar en cuenta:

• La red de datos debe ser administrada a través de un Sistema operativo de red fiable, seguro y debidamente actualizado en sus versiones y parches de seguridad.

• Deberán definirse políticas de roles, funciones y usuarios para el acceso a la red. Los recursos compartidos deben estar protegidos solo para personal autorizado.

• Disponer de herramientas de software que permitan monitorear alguna actividad sospechosa o inusual en la red o en las computadoras que pertenecen a ella.

Controles para evitar que existan ataques de "broadcast" en la red que pudieran hacer caer las conexiones.

• Establecer políticas de cambio de contraseñas de los usuarios de la red preferiblemente cada 30 días.

• Los accesos a las redes inalámbricas debe ser realizado validando usuario, contraseña y Mac Address del equipo. Se deberá permitir el acceso solo a los computadores de la Entidad.

• Se debe llevar bitácoras de registro de novedades, incidentes o eventos suscitados en la red de datos o comunicaciones.

• La información a través de las redes LAN y WAN de la Entidad deben viajar encriptados para evitar que puedan ser interceptadas e interpretadas.

• Se deberá disponer de suficientes controles de ancho de banda y calidad de servicio en los enlaces de transmisión de datos para la conexión entre el Servidor de Producción de base de datos y el de Standby ubicado en otra oficina.

• El acceso a internet debe ser administrado a través de un Servidor Proxy con suficientes restricciones para evitar la descarga de música y pornografía y acceso sólo a páginas relacionadas con el giro del negocio de la Entidad.

• Deben existir políticas para evitar la instalación de software ilegal o la inserción de dispositivos USB externos en las terminales de la red.

• Se deben implementar sistemas de control para evitar el SPAM o cualquier otro tipo de amenazas como virus, gusanos y troyanos. Se debe disponer de un Sistema de prevención de Intrusos.

• Los enlaces VPN deben estar controlados y monitoreados para garantizar su uso debido y deben ser habilitados solo cuando sea necesario y bajo la autorización del jefe de Seguridad o Jefe de Riesgos.

• Verificar que no existan puertos vulnerables y abiertos en los diferentes computadores personales, servidores u otros equipos conectados a la red que pudieran ocasionar una falla de seguridad.

• Realizar revisiones de “Ethical hacking” por lo menos una vez al año para verificar que no existan vulnerabilidades de la red a nivel interno y externo.

ANEXO 8. Manual de Procedimientos Unidad de la Auditoría Interna.

MANUAL DE PROCESOS YPROCEDIMIENTOS DE AUDITORÍA INTERNA

PRESENTACIÓN

El propósito del presente manual es proporcionar procedimientos y guías de trabajo para la ejecución de la auditoría a efecto de que se ajuste a métodos objetivos y sistemáticos que ayuden a mejorar las prácticas en la evaluación de la suficiencia, la eficacia, la eficiencia y la efectividad del control interno; así como facilitar las tareas del equipo de auditores.

El siguiente manual describe los procedimientos y/o lineamientos que debe seguir el personal de la Unidad de Auditoría Interna del Comisariato de la Policía Nacional en Masaya para llevar a cabo su trabajo, además de fortalecer la sistematización del trabajo

del auditor; con el presente manual se pretende que el mismo sea un mecanismo de capacitación para el personal que sea incorporado a la Unidad de Auditoría Interna, a fin de que se comprenda con mayor facilidad y claridad el trabajo a ejecutar.

I. INTRODUCCIÓN

La Auditoría Interna es una unidad operativa que tiene por finalidad el aseguramiento de ocurrencia mínima de riesgo y/o errores en las operaciones ejecutadas en la empresa, a través de la evaluación objetiva de evidencias y la generación de valor agregado mediante la emisión de recomendaciones que contribuyan a mejorar la gestión administrativa y alcanzar el logro de objetivos.

Ese proceso constituye una actividad independiente concebida para mejorar las operaciones; mediante la fiscalización periódica y el establecimiento de lineamientos para la aplicación de una metodología que permita el fortalecimiento del control interno de la empresa, que se observarán en la ejecución de los estudios de auditoría contenidos en el Plan Anual; así como el análisis de la información obtenida, formulación de hallazgos y comunicación de resultados.

II. OBJETIVO DEL MANUAL

El presente manual tiene por objetivo ser una herramienta de consulta permanente para todo el personal operativo de la Unidad de Auditoría Interna, y está dirigido a orientar las actividades de los auditores a fin de mejorar y unificar las prácticas y procedimientos utilizados en la ejecución de auditorías.

III- JUSTIFICACION DEL MANUAL

Los manuales de procesos y procedimientos, conforman uno de los elementos principales del Sistema de Control Interno; permitiendo un mayor desarrollo en la búsqueda del autocontrol, ya que dirige de manera sistemática la ejecución del trabajo que se realiza en la Unidad de Auditoría Interna.

El manual de procesos es una herramienta que permitirá a la Unidad de Auditoría Interna, integrar una serie de acciones encaminadas a agilizar el trabajo que se realiza; fomentando la calidad de las auditorías que se practiquen a través de lineamientos uniformes.

IV- ESTRUCTURA DEL MANUAL

a) Objeto y Alcance del Trabajo de Auditoría

El Objetivo de la Unidad de Auditoría Interna es brindar asesoría a la Máxima Autoridad de la empresa, para alcanzar el cumplimiento de las metas y objetivos; proporcionando análisis, evaluaciones y recomendaciones sobre las áreas sujetas a fiscalización y vigilando que las operaciones se ejecuten con transparencia y en apego a las disposiciones legales, asimismo promoviendo ante todo al personal de la empresa una cultura de respeto y cumplimiento a las leyes y procedimientos de control.

b) Alcance

Comprende la intervención y análisis de las operaciones que se ejecutan en la empresa, por medio de la evaluación de una Unidad, División, Departamento, Programa, Actividad, Proyecto, Producto, Proceso, Registro, Transacción, Contrato, etc., esto implica los resultados mensurables y evaluables de la eficacia, economía y eficiencia operacional que durante un período determinado se hayan producido, garantizando:

- ✓ El cabal cumplimiento a las disposiciones legales.
- ✓ La confiabilidad del sistema integrado de información contable financiera, administrativa y operativa.
- ✓ Los recursos se gestionen en forma eficiente y se protejan adecuadamente.
- ✓ Se identifiquen las áreas críticas de control, en las que se detecten mayores índices de riesgos.

c) Competencia de la Auditoría

A la Auditoría Interna le corresponde realizar actuaciones y auditorías, selectivas y posteriores que abarcan los aspectos presupuestarios, económicos, financieros, patrimoniales, normativos y de gestión; así como la evaluación de programas y proyectos, a través de un examen independiente, objetivo, sistemático y amplio del funcionamiento del control interno establecido en las operaciones y procesos internos de la empresa; realizando los siguientes tipos de auditorías:

Auditoría Financiera: Es aquella que emite un dictamen u opinión en relación con los estados financieros de la empresa.

Auditoría de Gestión: Es aquella que se enfoca en la gestión de la empresa con el propósito de evaluar la eficacia de los resultados con respecto a las metas previstas, los recursos humanos, financieros y técnicos utilizados en el cumplimiento de objetivos.

Auditoría de Cumplimiento Legal: Es aquella que se enmarca en la comprobación de que las operaciones financieras, administrativas, económicas y de otras índoles de la empresa se han realizado conforme a las normas legales y reglamentarias aplicables.

Auditorías Especiales: Son aquellas enfocadas de manera directa a una investigación específica, la importancia de esta auditoría radica en los hechos que originan la investigación.

d) ORGANIZACIÓN Y EJECUCIÓN DEL TRABAJO DE AUDITORÍA.

Plan General y Plan Operativo Anual

La Jefatura de la Unidad de Auditoría Interna realizará una planificación general y un plan anual de actividades a desarrollar por el equipo de auditores, el que será presentado a la

Máxima Autoridad de la empresa. El Plan General debe ser establecido para un (1) año; de este plan general se desprende el Plan Operativo Anual el cual tendrá que ser presentado en los primeros días de enero ambas planificaciones deberán ser revisadas y actualizadas si fuera necesario. Dicha planificación se elaborará en coordinación con la Jefatura de la Unidad y el equipo de auditores operativos.

Evaluación del Control Interno del Comisariato de la Policía Nacional de Masaya

La Unidad de Auditoría Interna debe evaluar el sistema de control interno implementado por la Administración; verificando que este permita salvaguardar los recursos, asegurar la exactitud y veracidad de la información financiera y administrativa, promover la eficiencia y calidad en las operaciones y lograr el cumplimiento de metas y objetivos programados; así como el cumplimiento de leyes y normas vigentes.

Para auditar la eficacia, eficiencia y efectividad del sistema de control interno, es importante tomar en cuenta los cinco componentes del control interno (Ambiente de Control, Evaluación y Gestión de Riesgos, Actividades de Control, Información y Comunicación, y Monitoreo del Control Interno empresa) los que están relacionados entre sí; para llevar a cabo dicha evaluación se utilizaran las técnicas y prácticas recomendadas, como ser entrevistas, cuestionarios, guías de análisis y
evaluación entre otras.

Organización y Ejecución del Trabajo de Auditoría

El Jefe de la Unidad de Auditoría Interna, asignará el trabajo mediante una orden de trabajo que contendrá las especificaciones necesarias para ejecutar la auditoría; así mismo se detallarán los objetivos generales y específicos, así como los rubros y período a auditar.
A la vez se deberá emitir la respectiva carta credencial, que es la que el auditor operativo presenta al auditado al momento de realizar el trabajo.

FASES DE LA AUDITORÍA.

Planeación:

- La primera tarea a cumplir dentro de la planificación de la auditoría es el reconocimiento del área sujeta a revisión, para lo cual será necesario recopilar la información necesaria acerca de las actividades a auditar, obteniendo una comprensión del sistema de control interno y sus procedimientos que permitirán desarrollar el plan respectivo considerando los riesgos inherentes de auditoría.

Se tomará como fuente de información:
01) El organigrama;
02) Las funciones asignadas;
03) Los objetivos y metas definidas;
04) La normativa jurídica y de administración;
05) Los manuales de procedimientos definidos;
06) La información obtenida a través de visitas a las distintas secciones, cuestionarios y entrevistas con el personal y

07) Toda otra información que se entienda pertinente.

- Se elabora la planificación general donde se determinan los objetivos, alcance de la auditoría, materiales a utilizar y la reglamentación legal aplicable.

- Se elabora el cuestionario de control interno, siendo este un análisis de vital importancia en esta etapa, ya que nos permitirá comprender la naturaleza del área auditada y del resultado que aquí se obtenga se considerará la extensión del plan de auditoría y la valoración y oportunidad de los procedimientos a utilizar durante el examen.

- Se realiza un análisis de riesgo de la auditoría, ya que puede representar que el auditor no detecte anomalía o exprese una opinión errónea por no considerar el mismo (riesgo inherente, de control y de detección).

- Se elabora el programa de auditoría; este es elaborado por el auditor que ha sido designado como Jefe de Equipo en coordinación con el Supervisor, dicho programa contiene las instrucciones y procedimientos que se emplearan en las diversas áreas de la auditoría; pueden ser modificados en la medida en que se ejecute el trabajo, teniendo en cuenta los hechos concretos que se vayan observando.

Ejecución:

- Durante esta fase se realizan diferentes tipos de pruebas y análisis para determinar la razonabilidad y/o detectar errores en las áreas sujetas a examen; se evalúan los resultados de las pruebas y se identifican los hallazgos, concluyendo con el trabajo asignado y emitiendo las recomendaciones respectivas que contribuirán a mejorar la gestión administrativa.

Las pruebas pueden ser de tres tipos: 1) Pruebas de Control, 2) Pruebas Analíticas,
3) Pruebas Sustantivas.

Se aplican diversas técnicas y/o procedimientos para encontrar las evidencias de auditoría que sustenten el informe.

Para la elección de los procedimientos y técnicas de auditoría, se tendrá en cuenta el resultado de la evaluación del Sistema de Control Interno realizado; dentro de los procedimientos que se pueden aplicar, tenemos:

Indagación: Consiste en la averiguación mediante entrevistas directas con el personal auditado o con terceros que tengan relación con las operaciones de ésta (evidencias testimoniales).

Encuestas y cuestionarios: Aplicación de preguntas relacionadas con las operaciones, para conocer la verdad de los hechos, situaciones u operaciones (evidencias documentales, testimoniales).

Observación: Verificación ocular de operaciones y procedimientos durante la ejecución de las actividades (evidencias físicas).

Revisión selectiva: Selección de las operaciones que serán evaluadas o verificadas en la ejecución de la auditoría (evidencias analíticas).

Revisión de cálculos matemáticos: Verificación de la exactitud aritmética de las operaciones contenidas en documentos (evidencias analíticas y documentales). Entre otros.

Adicionalmente podrán utilizarse métodos auxiliares que a criterio profesional del auditor y su experiencia considere necesarios según los riesgos y otras circunstancias, con vistas a obtener la evidencia necesaria y la suficiente certeza para sustentar sus conclusiones y opiniones de manera objetiva.

- Se evidencia el trabajo de auditoría; durante el desarrollo del examen el auditor debe evidenciar todo los hechos de importancia encontrados; la evidencia debe ser suficiente, competente y pertinente.

  Los tipos de evidencia pueden ser: Física, documental, evidencial, testimonial y analítica.

- Elaboración de papeles de trabajo; son los archivos o legajos que maneja el auditor y que contiene todos los documentos que sustentan el trabajo efectuado durante la auditoría.

Los papeles de trabajo revelan el alcance de la auditoría, la extensión y naturaleza de las pruebas aplicadas, por lo que su condición confidencial se mantiene durante el curso de la auditoría y después de realizada ésta, y deben archivarse con la seguridad que correspondan en la Unidad Auditoría Interna.

Entre los principales papeles se encuentran:

- Programa de auditoría;
- Cuestionarios o guías de control;
- Datos de la organización (organigramas y descripciones de puestos de trabajo);
- Copias de contratos y acuerdos importantes;
- Información sobre las políticas financieras y operativas;
- Resultados de las evaluaciones de los controles;
- Cartas de confirmación de saldos, comunicaciones y anotaciones;
- Copia del borrador del informe.

Los papeles de trabajo deberán ser elaborados:

- En forma simultánea a la aplicación de cada procedimiento, evitando postergar la anotación de la tarea realizada y de las eventuales observaciones;

- Facilitando la comprensión por quienes efectuarán la supervisión de la tarea, permitiendo la verificación precisa y rápida de que todos los procedimientos contenidos en el programa de trabajo se han cumplido.

Los papeles de trabajo se archivarán en carpetas que serán clasificadas como permanentes o corrientes.

- Se formulan los hallazgos encontrados en la auditoría; los hallazgos se consideran como diferencias significativas encontradas en el trabajo de auditoría con relación a lo normado o presentado por el auditado.

Los hallazgos deben tener los siguientes atributos:
1. Título.
2. Condición.
3. Criterio.
4. Causa.
5. Efecto.
6. Recomendación.

A pesar de que los hallazgos van implícitos en el informe de auditoría, estos también deben ser presentados en hojas individuales, con las fotocopias de la documentación que evidencie el hallazgo.

- Una vez concluido toda la labor de auditoría, se procede a referenciar los papeles de trabajo.

- Reunión con el auditado, previo a la culminación del informe se debe mantener una reunión con el responsable del área auditada a efectos de:

- Ponerlo en conocimiento de los hallazgos, conclusiones y recomendaciones de la auditoría previo a su remisión formal.

- Reducir el riesgo de interpretación errónea de los resultados, y

- Darle la oportunidad de realizar las aclaraciones pertinentes sobre los hallazgos de auditoría. Los comentarios que surjan en esta reunión deben ser tomados en cuenta, para la emisión del informe final.

Recepción de comentarios y emisión del primer informe

Elaboración del Informe
Una vez recibidos los comentarios efectuados por el, se emitirá el informe que será firmado por los integrantes de la comisión de auditoría y Jefe de la Unidad de Auditoría Interna.

- Una vez recibidos los comentarios efectuados por el responsable del área auditada; el Jefe de Equipo en coordinación con el equipo de auditores que practicaron la auditoría, proceden a elaborar el respectivo informe, que es el producto final del trabajo, por medio del cual se exponen las observaciones, conclusiones y recomendaciones.

- Una vez elaborado el informe por el equipo de auditores, este pasa a ser revisado por el supervisor y posteriormente por la Jefatura de la Unidad de Auditoría.

Comunicación y Notificación del Informe de Auditoría.

- ✓ El Jefe de la Unidad comunica la existencia del informe al Departamento de Supervisión de Auditorías Internas a la sede central de la Policía Nacional, para que procedan a la revisión del mismo.

- ✓ El o la supervisora del departamento de Auditorías Internas , procede a revisar el informe; si existen observaciones deben ser corregidas para ser revisadas nuevamente por el o la supervisora

.

- ✓ Una vez corregidas las mismas y/o de no existir observaciones , se da visto bueno por parte de el o la supervisora de la Departamento de Supervisión de Auditorías Internas de la Policía Nacional , para que el informe sea notificado.

Notificación del Informe
El informe que resultase de la auditoría, será notificado de la siguiente manera:

- Informe con Hallazgos de Control Interno.- una vez revisado y con visto bueno del área de Auditorías Internas de la Policía Nacional, se hará directamente a la Máxima Autoridad de la empresa.

Seguimiento de Recomendaciones:

El objetivo de toda auditoría es lograr que las recomendaciones emitidas sean implementadas por las autoridades competentes ya que ello dará como resultado mejoras en los niveles de eficacia, eficiencia y economía en la gestión administrativa de la empresa y al fortalecimiento del control interno.

Para dar seguimiento a las recomendaciones emitidas, se llevan a cabo las siguientes actividades:

- Se planifica el trabajo, para verificar el cumplimiento de las recomendaciones.

- Se ejecuta la auditoría del seguimiento a las recomendaciones.

- Se elabora el informe sobre las recomendaciones implementadas y los resultados que éstas dieron; así como las que no fueron acatadas y los impactos que estas produjeron por no implementarse.

- Se discute el informe con la Máxima Autoridad de la empresa, para dar a conocer los resultados del seguimiento y conocer las medidas que se tomaran al respecto.

- Se elabora el informe final.

- Se remite dicho informe a la Dirección de Auditorías Internas de la Policía Nacional y es este ente rector quien emitirá las sanciones correspondientes.

ANEXO No. 9
CÓDIGO DE ÉTICA DE LOS FUNCIONARIOS DE LA AUDITORIA INTERNA

Los funcionarios de la Auditoría Interna desarrollarán sus tareas de acuerdo con los siguientes principios y normas de conducta, además de los establecidos en las normativas vigentes:

1. Integridad.-

1.1. Los auditores internos desempeñarán su trabajo con honestidad, diligencia y responsabilidad.

1.2. Respetarán las leyes y divulgarán lo que corresponda de acuerdo con la ley.
No participarán a sabiendas de una actividad ilegal o ilícita.

1.3. Respetarán y contribuirán a los objetivos legítimos y éticos de la organización.

2. Objetividad.-

2.1. La actividad del auditor debe ejecutarse manteniendo independencia de criterio, desarrollando su trabajo con objetividad e imparcialidad en la formulación de los juicios.

2.2. La objetividad es una actitud mental independiente que deben mantener los auditores internos en la realización de sus trabajos. Deben tener una honesta confianza en el producto de su labor y en la calidad de la misma.

2.3. La objetividad consiste en una actuación fundada en la realidad de los hechos y circunstancias relevadas durante el plan de auditoría que permita mantener sobre bases sólidas las conclusiones y juicios sin deformación alguna.

2.4. Constituyen impedimentos internos o personales:
a) parentesco cercano por consanguinidad o afinidad.
b) amistad íntima o enemistad pública con aquellos cuya actividad debe evaluar.
c) intereses económicos relevantes con el ente evaluado.
d) prejuicios o favoritismos impulsados por razones políticas o religiosas.

2.5. Se debe comunicar a la Dirección cuando se verifiquen situaciones que comprometan la objetividad.

2.6. Los auditores deben proteger su independencia y evitar cualquier conflicto posible. Los auditores deben evitar toda clase de relaciones con las autoridades, directivos y personal del organismo auditado que puedan influir sobre, comprometer o amenazar la capacidad de los auditores para actuar y parecer que actúan con independencia.

2.7. Los auditores no deben participar en el diseño, implantación u operación de procedimientos o métodos de control.

3. Confidencialidad.-

3.1. Los auditores serán prudentes en el uso y protección de la información adquirida en el transcurso de su trabajo.

3.2. No utilizarán información para lucro personal o de cualquier forma que fuera contraria a la ley o en detrimento de los objetivos legítimos y éticos de la organización.

4. Competencia profesional.-

4.1. Los auditores deben conocer y cumplir las normas, las políticas, los procedimientos y las prácticas aplicables de auditoría, contabilidad y gestión presupuestal y financiera. Igualmente deben entender los principios y normas constitucionales, legales e institucionales que rigen el funcionamiento del organismo auditado.

4.2. El auditor efectuará las auditorias con el debido cuidado profesional. Esto supone que actuará aplicando la cautela, la reflexión y debida atención a las normas.

4.3. La actividad de AI debe reunir, en forma colectiva en el equipo, la pericia suficiente para cumplir con las responsabilidades asignadas:
a) Aptitud para la aplicación de normas,
b) Pericia en los principios y técnicas contables,
c) Conocimiento de las técnicas de identificación del fraude, técnicas de auditoría asistidas por computador (TAAC) y métodos cuantitativos,
d) Capacidad para comunicarse en forma oral y escrita de modo de transmitir eficazmente los objetivos, evaluaciones y conclusiones arribadas,
e) Cualidad para el trato con las personas,
f) Comprensión de los objetivos para evaluar la materialidad y significación de los hallazgos.

4.4. El debido cuidado implica prudencia y competencia razonable, no la infalibilidad ni una actuación extraordinaria. El debido cuidado requiere de exámenes, verificaciones y pruebas hasta un grado razonable.

4.5. Los auditores internos son responsables de continuar su formación a fin de mantener su competencia profesional. Deben mantenerse informados de las mejoras y evolución de las normas, procedimientos y técnicas de AI. La formación continua constituye una regla de conducta.

VIII. Bibliografía.

- ISACA COBIT3 y COBIT 4.0, disponible en http://www.solomanuales.org/curso-

- http://dmi.uib.es/~bbuades/auditoría/auditoría.PPT#266,11,Metodología (2)

- "Evaluación de los Sistemas de Tecnología Informática y Revisión de las Seguridades de Plataforma Específica para la empresa EMAPA-I"/ Andrea M. Tobar.

- Management Guidelines – Cobit 3rd Edition, Objetivos de Control Cobit, Resumen Ejecutivo Cobit, Marco Referencial Cobit, Implementation Tool Set – Cobit 3rd Edition

- Modelo Coso Report

- WHITTINGTON, O. Ray, PANY Kurt, Auditoría: Un enfoque Integral, Irwin McGrawHill, 12ª. Edición, Santa Fe de Bogota, Colombia, 2000

- Normas de Auditoría Interna emitidas por el The Institute of Internal Auditors

- Maldonado Milton, Auditoría de Gestión – Economía, Ecología, Eficacia, Eficiencia, Ética, 2001, disponible en http://www.monografias.com/trabajos14/auditoríasistemas/auditoríasistemas.shtml

- Auditoría Informática, Gonzalo Alonso Rivas, 1998 ediciones Díaz de Santos ISBN 84-87189-13.

- Auditoría en Informática Un enfoque metodológico y práctico, Lic. Enrique Hernández, 2002 editorial continental ISBN 970-24-0042-2.

- Auditoría informática, Piattini Velthuis Mario Gerardo y Del Peso Navarro Emilio, segunda edición.

- COBIT versión 4 disponible en:
- http://www.network-sec.com/COBIT_DS
- http://www.adacsi.org.ar/es/content.php
- http://www.reddeabastecimiento.org/COBIT%204.pdf

- "Evaluación de los Sistemas de Tecnología Informática y Revisión de las Seguridades de Plataforma Escuela Politécnica del Ejército para la empresa EMAPA-I"/ Andrea M. Tobar.