UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS ADMINISTRATIVAS Y HUMANÍSTICAS

CARRERA: CONTABILIDAD Y AUDITORÍA

TESIS DE GRADO

TEMA:

"AUDITORÍA INFORMÁTICA A LA SEGURIDAD FÍSICA EN LA DIVISIÓN REDES DE LA DIRECCIÓN NACIONAL DE TELECOMUNICACIONES E INFORMÁTICA DE LA CIUDAD DE QUITO AL PERIODO DEL 1 DE OCTUBRE DEL 2012 AL 31 DE ENERO DEL 2013"

Tesis presentada previa a la obtención del Título de Ingeniería en Contabilidad y Auditoría.

Autoras:

Bastidas Bonilla Susana Mercedes

Calero Yánez Ana Rocío

Director:

Dra. López Fraga Patricia Geraldina MSc.

Latacunga - Ecuador
Junio - 2015

AUTORÍA

Los criterios emitidos en el presente trabajo de investigación **"AUDITORÍA INFORMÁTICA A LA SEGURIDAD FÍSICA EN LA DIVISIÓN REDES DE LA DIRECCIÓN NACIONAL DE TELECOMUNICACIONES E INFORMÁTICA DE LA CIUDAD DE QUITO AL PERIODO DEL 1 DE OCTUBRE DEL 2012 AL 31 DE ENERO DEL 2013"**, son de exclusiva responsabilidad de los autores.

……	…….
Bastidas Bonilla Susana Mercedes	Calero Yánez Ana Rocío
C.I. 172217134-3	C.I. 050359487-1

AVAL DEL DIRECTOR DE TESIS

En calidad de Director del Trabajo de Investigación sobre el tema:

"AUDITORÍA INFORMÁTICA A LA SEGURIDAD FÍSICA EN LA DIVISIÓN REDES DE LA DIRECCIÓN NACIONAL DE TELECOMUNICACIONES E INFORMÁTICA DE LA CIUDAD DE QUITO AL PERIODO DEL 1 DE OCTUBRE DEL 2012 AL 31 DE ENERO DEL 2013", de Bastidas Bonilla Susana Mercedes y Calero Yánez Ana Rocío, postulantes de Ingeniería en Contabilidad y Auditoría, considero que dicho Informe Investigativo cumple con los requerimientos metodológicos y aportes científico-técnicos suficientes para ser sometidos a la evaluación del Tribunal de Validación de Tesis que el Honorable Consejo Académico de la **Unidad Académica de Ciencias Administrativas y Humanísticas de la Universidad Técnica de Cotopaxi** designe, para su correspondiente estudio y calificación.

Latacunga, junio del 2015

……

Dra. López Fraga Patricia Geraldina MSc.
C.I. 050220785-5
DIRECTORA DE TESIS

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de Miembros del Tribunal de Grado aprueban el presente Informe de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi, y por la Unidad Académica de Ciencias Administrativas y Humanísticas; por cuanto, los postulantes: Bastidas Bonilla Susana Mercedes y Calero Yánez Ana Rocío con el título de tesis: **"AUDITORÍA INFORMÁTICA A LA SEGURIDAD FÍSICA EN LA DIVISIÓN REDES DE LA DIRECCIÓN NACIONAL DE TELECOMUNICACIONES E INFORMÁTICA DE LA CIUDAD DE QUITO AL PERIODO DEL 1 DE OCTUBRE DEL 2012 AL 31 DE ENERO DEL 2013"** han considerado las recomendaciones emitidas oportunamente y reúne los méritos suficientes para ser sometido al acto de Defensa de Tesis.

Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional.

Latacunga, junio del 2015

Para constancia firman:

……	…….……..
Ing. Marcelo Cárdenas	Ing. Julio Salazar
PRESIDENTE	**MIEMBRO**

…….……

Ing. Patricio Bedón

OPOSITOR

AVAL DE LA DIRECCIÓN NACIONAL DE TELECOMUNICACIONES E INFORMÁTICA DE LA POLICÍA NACIONAL "DIVISIÓN REDES"

POLICIA NACIONAL
DIRECCION NACIONAL DE COMUNICACIONES
DIVISION REDES

CERTIFICACIÓN

Yo, Anchatipán Navas Danilo Fernando, Cabo Segundo de Policía, con C.I. 0502601974, en calidad de Administrador del Sistema Troncalizado de la División Redes de la Dirección Nacional de Comunicaciones de la Policía Nacional, certifico que las señoritas; Bastidas Bonilla Susana Mercedes con C.I. 172217134-3 y Calero Yánez Ana Rocío con C.I. 050359487-1; egresadas de la Universidad Técnica de Cotopaxi de la Carrera de Contabilidad y Auditoría, han concluido la **AUDITORÍA INFORMÁTICA A LA SEGURIDAD FÍSICA EN LA DIVISIÓN REDES DE LA DIRECCIÓN NACIONAL DE TELECOMUNICACIONES E INFORMÁTICA DE LA CIUDAD DE QUITO AL PERIODO DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2011.**

Dicho trabajo ha sido entregado y aprobado por todo el departamento, sujetándose a las Normas de Auditoría Generalmente Aceptadas.

Es todo cuanto puedo certificar, pudiendo las interesadas hacer uso lícito del presente documento como lo creyeren conveniente.

Quito, febrero del 2013

Tlgo. Danilo Fernando Anchatipán Navas.
Cabo Segundo de Policía
Administrador del Sistema Troncalizado

DEDICATORIA

Este trabajo de tesis de grado está dedicado a DIOS, por darme la vida a través de mis queridos PADRES quienes con mucho cariño, amor y ejemplo han hecho de mí una persona con valores para desenvolverme como: ESPOSA, MADRE Y PROFESIONAL.

A mi ESPOSO, que ha estado a mi lado dándome cariño, confianza y apoyo incondicional para seguir adelante.

A mis hijos Ethan y Daniela, que son el motivo y la razón que me ha llevado a seguir superándome día a día, quiero también dejar a cada uno de ellos una enseñanza que cuando se quiere alcanzar algo en la vida, no hay tiempo ni obstáculo que lo impida.

Susana

DEDICATORIA

A Dios, quien me dio la fe, la fortaleza, la salud y la esperanza para terminar este trabajo; por ser mi guía espiritual que me conduce siempre hacia el camino del bien y el éxito.

A mi madre Rosa Yánez por haberme educado, por el amor que siempre me ha brindado, por sembrar e inculcar ese sabio don de la responsabilidad y el respeto; gracias a usted hoy puede alcanzada mi meta.

A mi esposo Eduardo Oña, quien me brindo su amor, su cariño, su apoyo constante. Su comprensión y paciente espera para que pudiera terminar mi carrera son certeza de su gran amor.

Ana

AGRADECIMIENTO

Mi gratitud, principalmente está dirigida al Dios por haberme dado la existencia y permitido llegar al final de la carrera.

A los docentes que me han acompañado durante el largo camino, brindándome siempre su orientación con profesionalismo ético en la adquisición de conocimientos y afianzando mi formación.

A mis hermanos, cuñadas que de una u otra manera me han ayudado a cumplir mi sueño como es el caso de ser una profesional.

Susana

AGRADECIMIENTO

Hoy y siempre emitiere gratitud a Dios por darme la oportunidad de subir una grada más en el lapso de mi vida.

A mi madre por su gratitud eterna por sus bendiciones y sacrificio por cuidarme y darme siempre lo mejor.

A mi hija Génesis Doménica quien me prestó el tiempo que a ella le pertenecía por ella quiero ser cada día mejor y seguir siempre adelante. Gracias por existir en mi vida.

A la Dr. Patricia López por su acertada orientación en la elaboración y culminación de esta investigación.

Ana

ÍNDICE DE CONTENIDOS

CONTENIDOS *PÁGS.*

AUTORÍA ii

AVAL DEL DIRECTOR DE TESIS iii

APROBACIÓN DEL TRIBUNAL DE GRADO iv

AVAL DE LA DIRECCIÓN NACIONAL DE TELECOMUNICACIONES E INFORMÁTICA DE LA POLICÍA NACIONAL "DIVISIÓN REDES" v

DEDICATORIA vi

AGRADECIMIENTO viii

ÍNDICE DE CONTENIDOS x

ÍNDICE DE TABLAS xiv

ÍNDICE DE GRÁFICOS xv

RESUMEN xvi

SUMMARY xvii

AVAL DE TRADUCCIÓN xviii

INTRODUCCIÓN xix

CAPÍTULO I

FUNDAMENTACIÓN TEÓRICA DE UNA AUDITORÍA INFORMÁTICA A LA SEGURIDAD FÍSICA

1.1. Antecedentes Investigativos 1

1.2. Categorías Fundamentales 2

1.2.1. Gestión Administrativa y Financiera 3

1.2.1.1. Gestión Administrativa 3

1.2.1.2. Gestión Financiera 3

1.2.1.3. Función de la Gestión Administrativa – Financiera 4

1.2.2. Auditoría 5

1.2.2.1. Objetivo de la Auditoría 6

1.2.2.2. Clasificación de la Auditoría 6

1.2.3. Auditoría Informática 7

1.2.3.1. Objetivo de la Auditoría Informática 8

1.2.3.2. Importancia de la Auditoría Informática 9

1.2.3.3. Tipos de Auditoría Informática 9

1.2.3.4. Metodología para realizar una Auditoría Informática 11

1.2.3.5. Normas de Control Interno para la Auditoría Informática 12

1.2.4. Auditoría a la Seguridad Física 28

1.2.4.1. Objetivo Principal de Auditoría a la Seguridad Física 29

1.2.4.2. Instrumentos de Evaluación en la Auditoría de la Seguridad Física 29

1.2.4.3. Consideraciones de la Auditoría a la Seguridad Física 31

1.2.4.4. Tipos de Desastres en la Auditoría a la Seguridad Física 32

1.2.4.5. Metodología y fases de la Auditoría Informática a la Seguridad Física 34

1.2.4.5.1. Estudio Preliminar 35

1.2.4.5.2. Revisión y Evaluación de Controles y Seguridades: 35

1.2.4.5.3. Examen Detallado de Áreas Críticas: 36

1.2.4.5.4. Comunicación de Resultados 36

1.2.5. Papeles de Trabajo 38

1.2.5.1. Los objetivos de los Papeles de Trabajo son los siguientes: 39

1.2.5.2. Custodia y Archivo 40

1.2.5.3. Índices y Referencias 41

1.2.5.4. Marcas de Auditoría 42

CAPÍTULO II

MARCO INVESTIGATIVO

2. Breve Caracterización del Objeto de Estudio **33**
2.1. Reseña histórica **33**
2.1.1. Ubicación geográfica **34**
2.1.2. Misión **34**
2.1.3. Visión **34**
2.1.4. Objetivos organizacionales **34**
2.1.5. Estructura organizacional **36**
2.1.6. Funciones principales de la División Redes **37**
2.2. Diagnostico situacional de la institución **37**
2.2.1. Análisis Macroambiente **37**
2.2.2. Análisis Microambiente **39**
2.2.3. Análisis FODA **40**
2.3. Diseño Metodológico **41**
2.3.1. Tipo de Investigación **41**
2.3.2. Metodología **42**
2.3.3. Métodos de Investigación **42**
2.3.4. Técnicas de Investigación **43**
2.3.4.1. Observación **43**
2.3.4.2. Entrevista **43**
2.3.4.3. Encuesta.- **44**
2.4. Unidad de Estudio **44**
2.5. Preguntas Científicas **44**
2.6. Operacionalización de las Variables **46**
2.7. Entrevista al Coronel Jaime Jara Director Nacional de Telecomunicaciones e Informática de la P.N. **47**
2.8. Análisis de los resultados de la entrevista aplicada al Coronel Jaime Jara Director Nacional **49**
2.9. Entrevista al Jefe de la División Redes Mayor Giovanni Naranjo **50**
2.10. Análisis de los resultados de la entrevista aplicada al Jefe de la División Redes Mayor Giovanni Naranjo **52**
2.11. Análisis e interpretación de los resultados de las encuestas aplicadas al personal de la División Redes de la Dirección Nacional de Telecomunicaciones e Informática de la P.N. **53**
2.12. Conclusiones **67**
2.13. Recomendaciones **68**

CAPÍTULO III

"AUDITORÍA INFORMÁTICA A LA SEGURIDAD FÍSICA EN LA DIVISIÓN REDES DE LA DIRECCIÓN NACIONAL DE TELECOMUNICACIONES E INFORMÁTICA DE LA POLICÍA NACIONAL, DE LA CIUDAD DE QUITO, AL PERÍODO DEL 1 DE OCTUBRE DEL 2012 AL 31 DE ENERO DEL 2013"

3. Diseño de la Propuesta *69*

3.1. Introducción *69*

3.2. Justificación *70*

3.3. Objetivos *71*

3.3.1. Objetivo General *71*

3.3.2. Objetivos Específicos *71*

3.4 Descripción de la Propuesta *72*

3.5 Desarrollo de la propuesta *73*

3.5.1. Archivo Permanente *74*

3.6 Archivo Corriente *113*

3.6.1 Fase I Estudio Preliminar *114*

3.6.2 Fase II Revisión y Evaluación de Controles y Seguridades *136*

3.6.3 Fase III Examen Detallado de Áreas Críticas *161*

3.6.4. Comunicación de Resultados *189*

3.7 Plan de Mejora *200*

3.8. Conclusiones *201*

3.9. Recomendaciones *202*

3.10. Referencias Bibliográficas *203*

3.11. Anexos *205*

ÍNDICE DE TABLAS

CONTENIDOS ***PÁGS.***

TABLA 1. ANÁLISIS FODA.....41

TABLA 2. POBLACIÓN O UNIVERSO 44

TABLA 3. OPERACIONALIZACIÓN DE LAS VARIABLES.....46

TABLA 4. SEGURIDAD EN LA DIVISIÓN REDES.....53

TABLA 5. SALIDA DE EMERGENCIA 54

TABLA 6. INTERRUPTORES DE ENERGÍA ELÉCTRICA 55

TABLA 7. PREPARACIÓN DEL PERSONAL 56

TABLA 8. COPIAS DE LOS ARCHIVOS.....57

TABLA 9. PLAN DE CONTINGENCIA 58

TABLA 10. CABLES DE RED, SWITCH, HUBS.....59

TABLA 11. MANTENIMIENTO DE COMPUTADORAS.....60

TABLA 12. REGULADORES PARA EQUIPO DE CÓMPUTO.....61

TABLA 13. TIERRA FÍSICA.....62

TABLA 14. LUGAR SUFICIENTE PARA LOS EQUIPOS.....63

TABLA 15. PISO ANTIESTÁTICO.....64

TABLA 16. AIRE ACONDICIONADO 65

TABLA 17. TEMPERATURA EN QUE TRABAJAN LOS EQUIPOS.....66

ÍNDICE DE GRÁFICOS

CONTENIDOS ***PÁGS.***

GRÁFICO 1. CATEGORÍAS FUNDAMENTALES 2

GRÁFICO 2. EJEMPLO DE PAPELES DE TRABAJO 43

GRÁFICO 3. ORGANIGRAMA D.N.T.I. 36

GRÁFICO 4. SEGURIDAD EN LA DIVISIÓN REDES.....53

GRÁFICO 5. SALIDA DE EMERGENCIA 54

GRÁFICO 6. INTERRUPTORES DE ENERGÍA ELÉCTRICA 55

GRÁFICO 7. PREPARACIÓN DEL PERSONAL 56

GRÁFICO 8. COPIAS DE LOS ARCHIVOS.....57

GRÁFICO 9. PLAN DE CONTINGENCIA 58

GRÁFICO 10. CABLES DE RED, SWITCH, HUBS 59

GRÁFICO 11. MANTENIMIENTO DE COMPUTADORAS.....60

GRÁFICO 12. REGULADORES PARA EQUIPO DE CÓMPUTO.....61

GRÁFICO 13. TIERRA FÍSICA.....62

GRÁFICO 14. LUGAR SUFICIENTE PARA LOS EQUIPOS.....63

GRÁFICO 15. PISO ANTIESTÁTICO.....64

GRÁFICO 16. AIRE ACONDICIONADO 65

GRÁFICO 17. TEMPERATURA EN QUE TRABAJAN LOS EQUIPOS....66

UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS ADMINISTRATIVAS Y HUMANÍSTICAS

Latacunga – Ecuador

TEMA: "AUDITORÍA INFORMÁTICA A LA SEGURIDAD FÍSICA EN LA DIVISIÓN REDES DE LA DIRECCIÓN NACIONAL DE TELECOMUNICACIONES E INFORMÁTICA DE LA CIUDAD DE QUITO AL PERIODO DEL 1 DE OCTUBRE DEL 2012 AL 31 DE ENERO DEL 2013"

Autores:
Bastidas Bonilla Susana Mercedes
Calero Yánez Ana Rocío

RESUMEN

A pesar de que se invierte miles y en ocasiones millones de dólares en equipo de tecnología de punta para lograr los objetivos económicos que se propone una empresa, actualmente nos encontramos con que muchas organizaciones sufren de incidentes en donde se viola la Seguridad Física de sus instalaciones por terceros e inclusive por personal interno, esto posiblemente se debe, a que la Seguridad Física es en muchas ocasiones tomada como un elemento de "menor prioridad", sea por iniciativa orgánica o por omisión. La presente investigación determina la Metodología que se debe seguir para realizar la Auditoría a la Seguridad Física teniendo como un caso real la División Redes de la Dirección Nacional de Telecomunicaciones e Informática de la Policía Nacional. Mediante utilización de técnicas de investigación como son la encuesta, la entrevista y fichas de observación se obtuvo información concreta sobre la situación real de la empresa en cuanto al cumplimiento de normas de Seguridad. Además esta investigación fue de gran aporte a la Institución ya que se pudo señalar los inconvenientes existentes en cuánto al cumplimiento de normas, obteniendo como resultado de esta investigación nociones de una inadecuada aplicación de normas, las mismas que se ven reflejadas en los puntos de control interno y en el Informe Final de Auditoría.

TECHNICAL UNIVERSITY OF COTOPAXI

ACADEMIC CIENCE UNIT ADMINISTRATIVE AND HUMANITIES

Latacunga – Ecuador

THEME: "INFORMATIC AUDIT OF THE PHYSICAL SECURITY IN THE NETWORKS DIVISION OF THE NATIONAL MANAGEMENT OF TELECOMMUNICATIONS AND INFORMATICS OF THE CITY OF QUITO IN THE PERIOD OF OCTOBER 1ST OF 2012 TO JANUARY 31ST OF 2013"

Authors:
Bastidas Bonilla Susana Mercedes
Calero Yánez Ana Roció

SUMMARY

Although thousands and, on some occasions, millions of dollars are invested in technological equipment with the end of achieving economic objectives that a business proposes, at present we find that many organizations suffer from incidents where they violate the Physical Security of their installations by a third party and also by internal personnel, this must possibly be, that the Physical Security is in many cases taken as an element of "low priority", whether by organic initiative or by omission. The present investigation determines the Methodology that must be followed in order to realize the Audit of the Physical Security having as a real case the Networks Division of the National Management of Telecommunications and Informatics of the National Police. By means of utilizing investigative techniques such as the survey, interview, and observation records, concrete information is obtained about the real situation of a business in terms of the fulfillment of Security standards. In addition, this investigation was a great contribution to the Institution since the existing inconveniences could be pointed out in terms of the fulfillment of standards, obtaining as a result of this investigation notions of inadequate application of standards, the same that are reflected at points of internal control and in the Final Audit Report.

Universidad Técnica de Cotopaxi

CENTRO CULTURAL DE IDIOMAS

AVAL DE TRADUCCIÓN

En calidad de Docente del Idioma Inglés del Centro Cultural de Idiomas de la Universidad Técnica de Cotopaxi; en forma legal CERTIFICO que: La traducción del resumen de tesis al Idioma Inglés presentado por las señoritas Egresadas de la Carrera Ingeniería en Contabilidad y Auditoría de la Unidad Académica de Ciencias Administrativas y Humanísticas: **BASTIDAS BONILLA SUSANA MERCEDES Y CALERO YÁNEZ ANA ROCÍO**, cuyo título versa **"Auditoría Informática a la Seguridad Física en la División Redes de la Dirección Nacional de Telecomunicaciones e Informática de la ciudad de Quito al periodo del 1 de octubre del 2012 al 31 de enero del 2013"**, lo realizó bajo mi supervisión y cumple con una correcta estructura gramatical del Idioma.

Es todo cuanto puedo certificar en honor a la verdad y autorizo a las peticionarias hacer uso del presente certificado de la manera ética que estimaren conveniente.

Latacunga, junio del 2015

Atentamente,

Lic. M. Sc. Marcia Janeth Chiluisa Chiluisa
DOCENTE CENTRO CULTURAL DE IDIOMAS
C.C. 050221430-7

INTRODUCCIÓN

Las organizaciones pueden llegar a triunfar o a morir solamente por la información que manejan, lo que ha llevado a que ésta sea considerada como un activo cada vez más valioso, aun cuando no podemos llegar a cuantificarlo adecuadamente. Es muy importante ser consciente que por más que la División Redes sea la más segura desde el punto de vista de ataques externos (Hackers, virus, etc.); la seguridad de la misma será nula si no se ha previsto como combatir un incendio.

Existe actualmente dos elementos que incrementan la importancia de brindar una adecuada seguridad a la información corporativa por parte de las organizaciones: la importancia de la información para las organizaciones y el aumento de los riesgos que la misma se ve expuesta.

Con la aplicación de la Auditoría a la Seguridad Física se garantiza la confidencialidad, integridad y disponibilidad de la información; debido a que engloba todas las seguridades que debe tener un centro de datos.

El trabajo propuesto está estructurado de la siguiente manera:

Capítulo I, se establece la fundamentación teórica-conceptual, en base a la información recopilada de libros y páginas virtuales, que sustentan teorías esenciales para la aplicación de una Auditoría a la Seguridad Física en la División Redes de la Dirección Nacional de Telecomunicaciones e Informática de la Policía Nacional.

Capítulo II, se detalla el análisis e interpretación de los resultados para obtener información de la situación actual de la entidad. Esto se lo lleva a cabo a través de entrevistas realizadas al Coronel Jaime Jara y al Mayor Giovanni Naranjo. Además se aplica encuestas al personal técnico que labora en la Dirección Nacional de Telecomunicaciones e Informática “División Redes”. En base a la información recopilada se revalida la aplicación de la Auditoria a la Seguridad Física en esta institución.

Capítulo III, se enfoca en la aplicación de la Auditoría Informática a la Seguridad Física, donde se encuentra los papeles de trabajo con todos los hallazgos que son plasmados en el Informe Final de la Auditoría. El mismo que contiene conclusiones y recomendaciones que es entregada a la División Redes como aporte del grupo de investigación.

Finalmente, se encuentra las conclusiones y recomendaciones que la investigación genera.

CAPÍTULO I

FUNDAMENTACIÓN TEÓRICA DE UNA AUDITORÍA INFORMÁTICA A LA SEGURIDAD FÍSICA

1.1. Antecedentes Investigativos

En un ambiente donde la Informática está encabezando el trabajo en las diferentes oficinas e instituciones, el almacenamiento, ejecución y procesamiento de los datos se está haciendo vía computadoras, por lo tanto en el trabajo de la Auditoría también es algo indispensable. Aunque en el ambiente de la Informática la computadora es el medio principal para auditar pero no hay que olvidar que es a la persona junto a la información la cual estamos auditando y no la computadora en sí, no se cambió el espiritú de la Auditoría tradicional, solamente se cambió el método.

Se encontró en la tesis presentado por HIDALGO M, Braulio y URBINA B, Kléver; *Auditoría Informática a los laboratorios y sistemas (S.A.E. y Control Docente) de la FIS – UTA*, Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, (Ambato-Ecuador 2007). (Pág. 114,118). Según las observaciones de dicho proyecto se detalla que "no se cuenta con documentación de las aplicaciones, mantenimiento y seguros así como con los registros de averías o daños de los equipos, al igual que los inventarios de hardware y software no se encuentran debidamente actualizados". Por otra parte se menciona que "no existe un plan de contingencias para la red y no existe pólizas de seguro para los laboratorios".

Se halló además documentación en Internet de la Universidad Privada José Carlos Mariátegui; *Auditoría Informática Municipalidad Provincial Mariscal*, (Perú, 2004). (pág. 95-96). Y detalla que "el aspecto organizativo debe estar perfectamente estructurado, y las líneas de mando deben estar bien definidas, evitando de esta manera la rotación innecesaria de personal, la duplicidad de funciones, y que conllevan al desquiciamiento de la estructura organizacional".

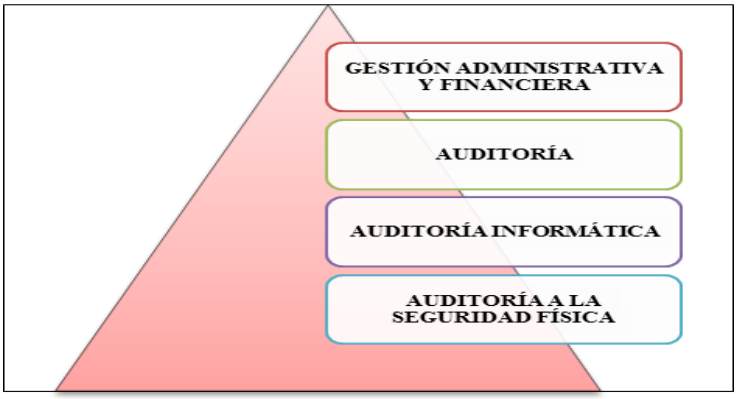
La seguridad de los computadores y de las instalaciones, así como de la información, el control de los accesos también es punto fundamental para evitar las pérdidas de información o manipulación indebida de esta.

Como resultado de la Auditoría Informática realizada a la Municipalidad Provincial Mariscal, determina que el área de Informática presenta deficiencias en: su Seguridad, área Física, Redes y en el debido cumplimiento de sus funciones.

Las postulantes mencionan que la realización de una Auditoria Informática puede contribuir a la detección de irregularidades y por ende a la toma de decisiones oportunas, sin riesgos materiales y económicos para la institución auditada.

1.2. Categorías Fundamentales

GRÁFICO 1. CATEGORÍAS FUNDAMENTALES



Fuente: Anteproyecto de tesis
Elaborado por: Las investigadoras

1.2.1. Gestión Administrativa y Financiera

La Gestión Administrativa y financiera son factores importantes que ayuda al buen desempeño de los administradores de toda organización.

1.2.1.1. Gestión Administrativa

En la Gestión Administrativa ha tomado mayor importancia con el pasar de tiempo, a medida que las actividades de las empresas crecen, su ejecución comprende la utilización de considerables reparticiones lo que obliga a los directivos a una administración técnica de sus recursos materiales, financiera, tecnológica, y de tiempo.

Según el autor CHIAVENATO, Idalverto, (2007), expresa que en la Gestión Administrativa: "el administrador es responsable del desempeño de una o más personas de la organización, el administrador obtiene resultados a través de la organización y de las personas que trabajan en ella, por consiguiente planea, organiza, dirige personas, gestiona y controla recursos materiales, financieros y tecnología para conseguir determinados objetivos" (Pág. 31).

Según REYES PONCE, Agustín (2004), manifiesta que, "la Gestión Administrativa es todo proceso administrativo en las que se fijan las metas de la entidad y de implementar las actividades para alcanzar los objetivos mediante el empleo eficiente de los recursos humanos, los materiales y el capital". (Pág. 2).

Por lo tanto las investigadoras manifiestan que la Gestión Administrativa en las empresas es un proceso donde se organiza, coordina y controla, utilizando de todos sus recursos para que de esa manera se pueda cumplir con cada uno de sus objetivos.

1.2.1.2. Gestión Financiera

A medida que las empresas crecen, también lo hacen los retos que supone la gestión de las finanzas. Sin una solución de Gestión Financiera integrada y automatizada, los procesos financieros y contables de la empresa pueden saturarse

a causa de la mayor complejidad del negocio, lo que originaría problemas de ineficiencia e imprecisión que podrían suponer la pérdida de oportunidades y de ingresos.

Según el autor FAINSTEIN, Héctor y ABADI Mauricio, (2009), menciona que, "se denomina Gestión Financiera (o gestión de movimiento de fondos) a todos los procesos que consisten en conseguir, mantener y utilizar dinero, sea físico (billetes y monedas) o a través de otros instrumentos, como cheques y tarjetas de crédito. La Gestión Financiera es la que convierte a la visión y misión en operaciones monetarias". (Pág. 45).

Según el autor MARTIN, Fernando (2002), expresa que la Gestión Financiera es***:*** "el conjunto de técnicas y actividades a dotar a una empresa de la estructura financiera idónea en función de sus necesidades mediante una adecuada planificación, elección y control, tanto en la obtención como en la utilización de los recursos financieros". (Pág. 113).

Las investigadoras consideran que la Gestión Financiera es la adquisición o manejo correcto de los fondos económicos de toda institución y así poder cumplir con los objetivos propuestos por cada una de las empresas, es decir, es la función financiera integra.

1.2.1.3. Función de la Gestión Administrativa – Financiera

Según el autor REYES, PONCE, Agustín (2004), indica que la función de la Gestión Administrativa - Financiera "es una empresa que se basa primordialmente en planear, adquirir y utilizar los fondos de tal forma que se incremente al máximo la eficiencia de las operaciones de la organización por lo tanto los administradores de la empresa e instituciones financieras juegan un papel muy importante, los mismos que deben considerar un gran número de fuentes y los usos alternativos para la correcta toma de decisiones". (Pág. 38).

1.2.2. Auditoría

Auditoría es un término que puede hacer referencia a tres cosas diferentes pero conectadas entre sí: puede referirse al trabajo que realiza un auditor, a la tarea de estudiar la economía de una empresa, o a la oficina donde se realizan estas tareas (donde trabaja el auditor). La actividad de auditar consiste en realizar un examen de los procesos y de la actividad económica de una organización para confirmar si se ajustan a lo fijado por las leyes o los buenos criterios.

Según MADARIAGA, Juan: (2004). La Auditoría en general, "es un examen sistemático de los Estados Financieros, registros y operaciones con la finalidad de determinar si están de acuerdo con los Principios de Contabilidad Generalmente Aceptados, con las políticas establecidas por la dirección y con cualquier otro tipo de exigencias legales o voluntariamente adoptadas" (pág. 13).

Según MENDIVI, Víctor: (2002). La Auditoría "es el proceso que efectúa un contador público independiente, al examinar los Estados Financieros preparados por una entidad económica, para reunir elementos de juicio suficientes, con el propósito de emitir una opinión profesional, sobre la credibilidad de dichos Estados Financieros, opinión que expresa en un documento formal denominado dictamen" (pág. 1).

Las postulantes consideran que la Auditoría es el examen crítico y sistemático que realiza una persona o grupo de personas profesionales independientes del sistema auditado, para emitir un informe técnico que ayudará en la toma de decisiones de la empresa.

Para entender de mejor manera e interpretar los objetivos de la Auditoría se ha tomado en cuenta según MADARIAGA, Juan; *Manual Práctico de Auditoría*; España; 2004, (Pág. 18).

1.2.2.1. Objetivo de la Auditoría

La Auditoría tiene por objeto averiguar la exactitud, integridad y autenticidad de los Estados Financieros, expedientes y demás documentos administrativos-contables presentados por la dirección, así como sugerir las mejoras que procedan.

Las postulantes manifiestan que la Auditoría es el proceso de acumular y evaluar evidencia, realizado por una persona independiente y competente acerca de la información cuantificable de una entidad económica específica, con el propósito de determinar e informar sobre el grado de correspondencia existente entre la información cuantificable y los criterios establecidos.

Para entender de mejor manera e interpretar la clasificación de la Auditoría se ha tomado en cuenta según PEÑA, Jesús; *Control, Auditoría y Revisión Física*; Colombia; 2007; (Pág. 46).

1.2.2.2. Clasificación de la Auditoría

Según sea realizada por personal vinculado o no laboralmente a la empresa, la Auditoría puede clasificarse en dos más grande ramas:

Auditoría Externa: Conocida también independiente, centra tradicionalmente su labor hacia los Estados Financieros con el fin de emitir un dictamen sobre su razonabilidad, aportando credibilidad por el análisis que de estos hace un profesional ajeno a la empresa que los preparar, los cuales una vez estudiados y evaluados son dictaminados.

Auditoría Interna: Es desarrollada por un personal vinculado laboralmente a la institución aunque al más alto nivel, con el fin de garantizar un análisis objetivo e independiente de lo examinado.

Auditoría Financiera: Tiene como objetivo el examen y evaluación de los saldos y su presentación en los Estados Financieros, para dictaminar la razonabilidad de estos con base en normas de Auditoría de aceptación general tanto internacional como nacional. Para el desarrollo de esta Auditoría se apoya en la Auditoría

Operativa y en la evaluación del Control Interno que le permite formarse un concepto sobre las necesidades del alcance de las pruebas a efectuar y procedimientos a aplicar.

Auditoría Administrativa: Comprende el examen del establecimiento y el cumplimiento de los planes, políticas, metas y objetivos trazados por la dirección general, en todas las fases del proceso administrativo: planeación, organización, dirección y control.

Auditoría de Cumplimiento: Ejerce el control posterior o consecutivo sobre la aplicación de la normatividad existente para el manejo empresarial, registros contables, presentación de los Estados Financieros.

Auditoría Informática: Se conoce también como Auditoría de Sistemas, teniendo como objetivo evaluar el sistema informático en forma integral, los procedimientos y seguridad de los equipos electrónicos o hardware, de los programas o software que posee la empresa, sean propios o en modalidad de servicios.

Auditoría de Gestión: Conocida como de resultado, comprueba la eficacia administrativa en el coordinado manejo de los recursos para el logro de los objetivos y metas previamente determinados.

Tomando en consideración todas las investigaciones realizadas, las postulantes manifiestan que la Auditoría es dinámica, la cual debe aplicarse formalmente toda empresa, independientemente de su magnitud y objetivos; aun en empresas pequeñas, en donde se llega a considerar inoperante, su aplicación debe ser secuencial constatada para lograr eficiencia.

1.2.3. Auditoría Informática

La Auditoría Informática ha sido erróneamente denominada Auditoría de Sistemas, por el hecho que vulgarmente se considera la palabra "sistemas" como sinónimo de "computador". Pero a lo largo de lo desarrollado hasta el momento,

ha quedado claro que toda Auditoría es de Sistemas, pues su objeto son los Sistemas de Información.

Según ECHENIQUE, José A; (2002). La Auditoría Informática es "la revisión y evaluación de los controles, sistemas y procedimientos de la Informática; de los equipos de cómputo, su utilización, eficiencia y seguridad; de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente, confiable y segura de la información que servirá para una adecuada toma de decisiones" (Pág. 18).

Según el ingeniero diplomado CASTRO, Julián, (2003). Auditoría Informática es "La verificación de controles en el procesamiento de la información, instalada, con el objeto de evaluarlos y presentar recomendaciones a gerencia" (Pág. 17).

Las investigadoras consideran que la Auditoría Informática es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una empresa con respecto los Sistemas de Información. Además es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo empresarial, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas.

Para lograr un mejor análisis e interpretación de lo que significa los objetivos de Auditoría Informática se ha tomado en cuenta según RIVAS, *Gonzalo; Auditoría Informática*; España; 1988; (Pág. 41).

1.2.3.1. Objetivo de la Auditoría Informática

- Uso eficiente y eficaz de protección y control de los Elementos informáticos. Este objetivo pone énfasis en los elementos informáticos (TI blandas y duras).

- Protección del patrimonio de la empresa. Esto se logra con buena información de apoyo para la planificación y control de los activos, así como a las funciones financieras.

- Alineamiento de la información a las áreas críticas del negocio para lograr los objetivos. Este es el objetivo más general y relevante.

Las postulantes mencionan que dentro de una Auditoría Informática se debe cumplir ciertos objetivos que ayudará en la planificación del trabajo institucional y la toma de decisiones más confiable.

Para lograr un mejor análisis e interpretación de lo que significa la importancia y los tipos de la Auditoría Informática se tomó en cuenta la definición según: *http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica/11:20/10-10-2012.*

1.2.3.2. Importancia de la Auditoría Informática

La Auditoría permite a través de una revisión independiente, la evaluación de actividades, funciones específicas, resultados u operaciones de una organización, con el fin de evaluar su correcta realización. Este autor hace énfasis en la revisión independiente, debido a que el auditor debe mantener independencia mental, profesional y laboral para evitar cualquier tipo de influencia en los resultados de la misma.

La técnica de la Auditoría, siendo por tanto aceptables equipos multidisciplinarios formados por titulados en Ingeniería Informática e Ingeniería Técnica en Informática y licenciados en derecho especializados en el mundo de la auditoría.

1.2.3.3. Tipos de Auditoría Informática

Dentro de la Auditoría Informática destacan los siguientes tipos (entre otros):

Auditoría de la Gestión: la contratación de bienes y servicios, documentación de los programas, etc.

Auditoría Legal del Reglamento de Protección de Datos: Cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos.

Auditoría de los Datos: Clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.

Auditoría de las Bases de Datos: Controles de acceso, de actualización, de integridad y calidad de los datos.

Auditoría de la Seguridad: Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.

Auditoría de la Seguridad Física: Referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta. También está referida a las protecciones externas (arcos de seguridad, CCTV, vigilantes, etc.) y protecciones del entorno.

Auditoría de la Seguridad Lógica: Comprende los métodos de autenticación de los Sistemas de Información.

Auditoría de las Comunicaciones: Se refiere a la Auditoría de los procesos de autenticación en los sistemas de comunicación.

Auditoría de la Seguridad en Producción: Frente a errores, accidentes y fraudes.

Las postulantes mencionan que la Auditoría Informática es importante ya que permite a través de una revisión independiente, la evaluación de actividades, funciones específicas, de una organización, conlleva a la toma de decisiones oportunas para el bienestar institucional.

Para lograr un mejor análisis e interpretación de lo que significa la metodología de la Auditoría Informática se ha tomado en cuenta según RIVAS, *Gonzalo; Auditoría Informática*; España; 1988, (Pág. 47).

1.2.3.4. Metodología para realizar una Auditoría Informática

Existen algunas metodologías de Auditoría de Sistemas y todas dependen de lo que se pretenda revisar o analizar, pero como estándar, las cuatro fases básicas en un proceso de revisión son:

Fases de un proceso de Auditoría:

- ✓ Estudio preliminar
- ✓ Revisión y evaluación de controles y seguridades
- ✓ Examen detallado de áreas criticas
- ✓ Comunicación de resultados

Estudio Preliminar: Incluye definir el grupo de trabajo, el programa de Auditoría, efectuar visitas a la unidad informática para conocer detalles de la misma, elaborar un cuestionario para la obtención de información para evaluar preliminarmente el Control Interno, solicitud de plan de actividades, Manuales de políticas, Reglamentos, entrevistas con los principales funcionarios del PAD.

Revisión y Evaluación de Controles y Seguridades: Consiste en la revisión de los diagramas de flujo de procesos, realización de pruebas de cumplimiento de las seguridades, revisión de aplicaciones de las áreas críticas, revisión de procesos históricos (backups), revisión de documentación y archivos, entre otras actividades.

Examen Detallado de Áreas Críticas: Con las fases anteriores el auditor descubre las áreas críticas y sobre ellas hace un estudio y análisis profundo en los que definirá concretamente su grupo de trabajo y la distribución de carga del mismo, establecerá los motivos, objetivos, alcance recursos que usara, definirá la metodología de trabajo, la duración de la Auditoría, presentará el plan de trabajo y analizara detalladamente cada problema encontrado.

Comunicación de Resultados: Se elaborará el borrador del informe a ser discutido con los ejecutivos de la empresa hasta llegar al informe definitivo, el cual presentará esquemáticamente en forma de matriz, cuadros o redacción simple y concisa que destaque los problemas encontrados, los efectos y las recomendaciones de la Auditoría. El informe debe contener lo siguiente:

- ✓ Motivos de la Auditoría
- ✓ Objetivos
- ✓ Alcance
- ✓ Estructura Orgánico-Funcional del área Informática
- ✓ Configuración del Hardware y Software instalado
- ✓ Control Interno
- ✓ Resultados de la Auditoría

Las postulantes manifiestan que las organizaciones informáticas forman parte de lo que se ha denominado el "management" o gestión de la empresa. Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, desde el momento en que es una herramienta adecuada de colaboración. En este sentido y debido a su importancia en el funcionamiento de una empresa, existe la Auditoria Informática.

1.2.3.5. Normas de Control Interno para la Auditoría Informática

En este tema, tomamos como base las Normas de Control Interno de la Contraloría General de Estado, ya que estas son de obligatoriedad para las instituciones del sector público y sirven como marco de referencia para las instituciones y organizaciones a nivel privado para adoptar puntos referentes de evaluación y control de sus procesos.

Dentro del grupo 400, subgrupo 410 y en el grupo 500, encontramos las normas para la evaluación del control interno en el área de la Informática.

Así, las normas emitidas por la Contraloría General del Estado referente a Sistemas de Información y Comunicación son:

410.- Tecnología de la información

500.- Información y comunicación

410 TECNOLOGÍA DE LA INFORMACIÓN

410-01 Organización informática

Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional. La unidad de tecnología de información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo. Las entidades u organismos del sector público, establecerán una estructura organizacional de tecnología de información que refleje las necesidades institucionales, la cual debe ser revisada de forma periódica para ajustar las estrategias internas que permitan satisfacer los objetivos planteados y soporten los avances tecnológicos. Bajo este esquema se dispondrá como mínimo de áreas que cubran proyectos tecnológicos, infraestructura tecnológica y soporte interno y externo de ser el caso, considerando el tamaño de la entidad y de la unidad de tecnología.

410-02 Segregación de funciones

Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo. La asignación de

funciones y sus respectivas responsabilidades garantizarán una adecuada segregación, evitando funciones incompatibles. Se debe realizar dentro de la unidad de tecnología de información la supervisión de roles y funciones del personal dentro de cada unas de las áreas, para gestionar un adecuado rendimiento y evaluar las posibilidades de reubicación e incorporación de nuevo personal. La descripción documentada y aprobada de los puestos de trabajo que conforman la unidad de tecnología de información, contemplará los deberes y responsabilidades, así como las habilidades y experiencia necesarias en cada posición, a base de las cuales se realizará la evaluación del desempeño. Dicha descripción considerará procedimientos que eliminen la dependencia de personal clave.

410–03 Plan informático estratégico de tecnología

La unidad de tecnología de la información elaborará e implementará un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos, el mismo que estará alineado con el plan estratégico institucional y éste con el Plan Nacional de Desarrollo y las políticas públicas de gobierno. El plan informático estratégico tendrá un nivel de detalle suficiente para permitir la definición de planes operativos de tecnología de Información y especificará como ésta contribuirá a los objetivos estratégicos de la organización; incluirá un análisis de la situación actual y las propuestas de mejora con la participación de todas las unidades de la organización, se considerará la estructura interna, procesos, infraestructura, comunicaciones, aplicaciones y servicios a brindar, así como la definición de estrategias, riesgos, cronogramas, presupuesto de la inversión y operativo, fuentes de financiamiento y los requerimientos legales y regulatorios de ser necesario. La unidad de tecnología de información elaborará planes operativos de tecnología de la información alineados con el plan estratégico informático y los objetivos estratégicos de la institución, estos planes incluirán los portafolios de proyectos y de servicios, la arquitectura y dirección tecnológicas, las estrategias de migración, los aspectos de contingencia de los componentes de la infraestructura y consideraciones relacionadas con la incorporación de nuevas tecnologías de información vigentes a fin de evitar la obsolescencia. Dichos

planes asegurarán que se asignen los recursos apropiados de la función de servicios de tecnología de información a base de lo establecido en su plan estratégico. El plan estratégico y los planes operativos de tecnología de información, así como el presupuesto asociado a éstos serán analizados y aprobados por la máxima autoridad de la organización e incorporados al presupuesto anual de la organización; se actualizarán de manera permanente, además de ser monitoreados y evaluados en forma trimestral para determinar su grado de ejecución y tomar las medidas necesarias en caso de desviaciones.

410-04 Políticas y procedimientos

La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria. La unidad de tecnología de información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran. Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, serán considerados dentro de las políticas y procedimientos a definir, los cuales además, estarán alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información.

Será necesario establecer procedimientos de comunicación, difusión y coordinación entre las funciones de tecnología de información y las funciones propias de la organización. Se incorporarán controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos. Se implantarán procedimientos de supervisión de las funciones de tecnología de información, ayudados de la revisión de indicadores de desempeño

y se medirá el cumplimiento de las regulaciones y estándares definidos. La unidad de tecnología de información deberá promover y establecer convenios con otras organizaciones o terceros a fin de promover y viabilizar el intercambio de información interinstitucional, así como de programas de aplicación desarrollados al interior de las instituciones o prestación de servicios relacionados con la tecnología de información.

410-05 Modelo de información organizacional

La unidad de tecnología de información definirá el modelo de información de la organización a fin de que se facilite la creación, uso y compartición de la misma; y se garantice su disponibilidad, integridad, exactitud y seguridad sobre la base de la definición e implantación de los procesos y procedimientos correspondientes. El diseño del modelo de información que se defina deberá constar en un diccionario de datos corporativo que será actualizado y documentado de forma permanente, incluirá las reglas de validación y los controles de integridad y consistencia, con la identificación de los sistemas o módulos que lo conforman, sus relaciones y los objetivos estratégicos a los que apoyan a fin de facilitar la incorporación de las aplicaciones y procesos institucionales de manera transparente. Se deberá generar un proceso de clasificación de los datos para especificar y aplicar niveles de seguridad y propiedad.

410-06 Administración de proyectos tecnológicos

La unidad de tecnología de información definirá mecanismos que faciliten la administración de todos los proyectos informáticos que ejecuten las diferentes áreas que conformen dicha unidad. Los aspectos a considerar son:

1. Descripción de la naturaleza, objetivos y alcance del proyecto, su relación con otros proyectos institucionales, sobre la base del compromiso, participación y aceptación de los usuarios interesados.

2. Cronograma de actividades que facilite la ejecución y monitoreo del proyecto que incluirá el talento humano (responsables), tecnológicos y financieros además de los planes de pruebas y de capacitación correspondientes.

3. La formulación de los proyectos considerará el Costo Total de Propiedad CTP; que incluya no sólo el costo de la compra, sino los costos directos e indirectos, los beneficios relacionados con la compra de equipos o programas informáticos, aspectos del uso y mantenimiento, formación para el personal de soporte y usuarios, así como el costo de operación y de los equipos o trabajos de consultoría necesarios.

4. Para asegurar la ejecución del proyecto se definirá una estructura en la que se nombre un servidor responsable con capacidad de decisión y autoridad y administradores o líderes funcionales y tecnológicos con la descripción de sus funciones y responsabilidades.

5. Se cubrirá, como mínimo las etapas de: inicio, planeación, ejecución, control, monitoreo y cierre de proyectos, así como los entregables, aprobaciones y compromisos formales mediante el uso de actas o documentos electrónicos legalizados.

6. El inicio de las etapas importantes del proyecto será aprobado de manera formal y comunicado a todos los interesados.

7. Se incorporará el análisis de riesgos. Los riesgos identificados serán permanentemente evaluados para retroalimentar el desarrollo del proyecto, además de ser registrados y considerados para la planificación de proyectos futuros.

8. Se deberá monitorear y ejercer el control permanente de los avances del proyecto.

9. Se establecerá un plan de control de cambios y un plan de aseguramiento de calidad que será aprobado por las partes interesadas.

10. El proceso de cierre incluirá la aceptación formal y pruebas que certifiquen la calidad y el cumplimiento de los objetivos planteados junto con los beneficios obtenidos.

410-07 Desarrollo y adquisición de software aplicativo

La unidad de tecnología de información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos. Los aspectos a considerar son:

1. La adquisición de software o soluciones tecnológicas se realizarán sobre la base del portafolio de proyectos y servicios priorizados en los planes estratégico y operativo previamente aprobados considerando las políticas públicas establecidas por el Estado, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada.

2. Adopción, mantenimiento y aplicación de políticas públicas y estándares internacionales para: codificación de software, nomenclaturas, interfaz de usuario, interoperabilidad, eficiencia de desempeño de sistemas, escalabilidad, validación contra requerimientos, planes de pruebas unitarias y de integración.

3. Identificación, priorización, especificación y acuerdos de los requerimientos funcionales y técnicos institucionales con la participación y aprobación formal de las unidades usuarias. Esto incluye, tipos de usuarios, requerimientos de: entrada, definición de interfaces, archivo, procesamiento, salida, control, seguridad, plan de pruebas y trazabilidad o pistas de auditoría de las transacciones en donde aplique.

4. Especificación de criterios de aceptación de los requerimientos que cubrirán la definición de las necesidades, su factibilidad tecnológica y económica, el análisis de riesgo y de costo-beneficio, la estrategia de desarrollo o compra del software de aplicación, así como el tratamiento que se dará a aquellos procesos de emergencia que pudieran presentarse.

5. En los procesos de desarrollo, mantenimiento o adquisición de software aplicativo se considerarán: estándares de desarrollo, de documentación y de calidad, el diseño lógico y físico de las aplicaciones, la inclusión apropiada de controles de aplicación diseñados para prevenir, detectar y corregir errores e irregularidades de procesamiento, de modo que éste, sea exacto, completo, oportuno, aprobado y auditable. Se considerarán mecanismos de autorización, integridad de la información, control de acceso, respaldos, diseño e implementación de pistas de auditoría y requerimientos de seguridad. La especificación del diseño considerará las arquitecturas tecnológicas y de información definidas dentro de la organización.

6. En caso de adquisición de programas de computación (paquetes de software) se preverán tanto en el proceso de compra como en los contratos respectivos, mecanismos que aseguren el cumplimiento satisfactorio de los requerimientos de la entidad. Los contratos tendrán el suficiente nivel de detalle en los aspectos técnicos relacionados, garantizar la obtención de las licencias de uso y/o servicios, definir los procedimientos para la recepción de productos y documentación en general, además de puntualizar la garantía formal de soporte, mantenimiento y actualización ofrecida por el proveedor.

7. En los contratos realizados con terceros para desarrollo de software deberá constar que los derechos de autor será de la entidad contratante y el contratista entregará el código fuente. En la definición de los derechos de autor se aplicarán las disposiciones de la Ley de Propiedad Intelectual. Las excepciones serán técnicamente documentadas y aprobadas por la máxima autoridad o su delegado.

8. La implementación de software aplicativo adquirido incluirá los procedimientos de configuración, aceptación y prueba personalizados e implantados. Los aspectos a considerar incluyen la validación contra los términos contractuales, la arquitectura de información de la organización, las aplicaciones existentes, la interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos, la eficiencia en el desempeño del sistema, la documentación y los manuales de usuario, integración y planes de prueba del sistema.

9. Los derechos de autor del software desarrollado a la medida pertenecerán a la entidad y serán registrados en el organismo competente. Para el caso de software adquirido se obtendrá las respectivas licencias de uso.

10. Formalización con actas de aceptación por parte de los usuarios, del paso de los sistemas probados y aprobados desde el ambiente de desarrollo/prueba al de producción y su revisión en la post-implantación.

11. Elaboración de manuales técnicos, de instalación y configuración; así como de usuario, los cuales serán difundidos, publicados y actualizados de forma permanente.

410-08 Adquisiciones de infraestructura tecnológica

La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la organización para lo cual se considerarán los siguientes aspectos:

1. Las adquisiciones tecnológicas estarán alineadas a los objetivos de la organización, principios de calidad de servicio, portafolios de proyectos y servicios, y constarán en el plan anual de contrataciones aprobado de la institución, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada.

2. La unidad de tecnología de información planificará el incremento de capacidades, evaluará los riesgos tecnológicos, los costos y la vida útil de la inversión para futuras actualizaciones, considerando los requerimientos de carga de trabajo, de almacenamiento, contingencias y ciclos de vida de los recursos tecnológicos. Un análisis de costo beneficio para el uso compartido de Data Center con otras entidades del sector público, podrá ser considerado para optimizar los recursos invertidos.

3. En la adquisición de hardware, los contratos respectivos, tendrán el detalle suficiente que permita establecer las características técnicas de los principales componentes tales como: marca, modelo, número de serie, capacidades, unidades

de entrada/salida, entre otros, y las garantías ofrecidas por el proveedor, a fin de determinar la correspondencia entre los equipos adquiridos y las especificaciones técnicas y requerimientos establecidos en las fases precontractual y contractual, lo que será confirmado en las respectivas actas de entrega/recepción.

4. Los contratos con proveedores de servicio incluirán las especificaciones formales sobre acuerdos de nivel de servicio, puntualizando explícitamente los aspectos relacionados con la seguridad y confidencialidad de la información, además de los requisitos legales que sean aplicables. Se aclarará expresamente que la propiedad de los datos corresponde a la organización contratante.

410-09 Mantenimiento y control de la infraestructura tecnológica

La unidad de tecnología de información de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades. Los temas a considerar son:

1. Definición de procedimientos para mantenimiento y liberación de software de aplicación por planeación, por cambios a las disposiciones legales y normativas, por corrección y mejoramiento de los mismos o por requerimientos de los usuarios.

2. Los cambios que se realicen en procedimientos, procesos, sistemas y acuerdos de servicios serán registrados, evaluados y autorizados de forma previa a su implantación a fin de disminuir los riesgos de integridad del ambiente de producción. El detalle e información de estas modificaciones serán registrados en su correspondiente bitácora e informados a todos los actores y usuarios finales relacionados, adjuntando las respectivas evidencias.

3. Control y registro de las versiones del software que ingresa a producción.

4. Actualización de los manuales técnicos y de usuario por cada cambio o mantenimiento que se realice, los mismos que estarán en constante difusión y publicación.

5. Se establecerán ambientes de desarrollo/pruebas y de producción independientes; se implementarán medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos y garantizar su integridad y disponibilidad a fin de proporcionar una infraestructura de tecnología de información confiable y segura.

6. Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.

7. Se mantendrá el control de los bienes informáticos a través de un inventario actualizado con el detalle de las características y responsables a cargo, conciliado con los registros contables.

8. El mantenimiento de los bienes que se encuentren en garantía será proporcionado por el proveedor, sin costo adicional para la entidad.

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas:

1. Ubicación adecuada y control de acceso físico a la unidad de tecnología de información y en especial a las áreas de: servidores, desarrollo y bibliotecas;

2. Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado;

3. En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación;

4. Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización;

5. Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados.

6. Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire contralado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros;

7. Consideración y disposición de sitios de procesamiento alternativos.

8. Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana.

410-11 Plan de contingencias

Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado. Los aspectos a considerar son:

1. Plan de respuesta a los riesgos que incluirá la definición y asignación de roles críticos para administrar los riesgos de tecnología de información, escenarios de contingencias, la responsabilidad específica de la seguridad de la información, la seguridad física y su cumplimiento.

2. Definición y ejecución de procedimientos de control de cambios, para asegurar que el plan de continuidad de tecnología de información se mantenga actualizado y refleje de manera permanente los requerimientos actuales de la organización.

3. Plan de continuidad de las operaciones que contemplará la puesta en marcha de un centro de cómputo alterno propio o de uso compartido en un data Center Estatal, mientras dure la contingencia con el restablecimiento de las comunicaciones y recuperación de la información de los respaldos.

4. Plan de recuperación de desastres que comprenderá:

- ✓ Actividades previas al desastre (bitácora de operaciones)
- ✓ Actividades durante el desastre (plan de emergencias, entrenamiento)
- ✓ Actividades después del desastre.

5. Es indispensable designar un comité con roles específicos y nombre de los encargados de ejecutar las funciones de contingencia en caso de suscitarse una emergencia.

6. El plan de contingencias será un documento de carácter confidencial que describa los procedimientos a seguir en caso de una emergencia o fallo computacional que interrumpa la operatividad de los sistemas de información. La aplicación del plan permitirá recuperar la operación de los sistemas en un nivel aceptable, además de salvaguardar la integridad y seguridad de la información.

7. El plan de contingencias aprobado, será difundido entre el personal responsable de su ejecución y deberá ser sometido a pruebas, entrenamientos y evaluaciones periódicas, o cuando se haya efectuado algún cambio en la configuración de los equipos o el esquema de procesamiento.

410-12 Administración de soporte de tecnología de información

La unidad de tecnología de información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen. Los aspectos a considerar son:

1. Revisiones periódicas para determinar si la capacidad y desempeño actual y futura de los recursos tecnológicos son suficientes para cubrir los niveles de servicio acordados con los usuarios.

2. Seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad.

3. Estandarización de la identificación, autenticación y autorización de los usuarios, así como la administración de sus cuentas.

4. Revisiones regulares de todas las cuentas de usuarios y los privilegios asociados a cargo de los dueños de los procesos y administradores de los sistemas de tecnología de información.

5. Medidas de prevención, detección y corrección que protejan a los sistemas de información y a la tecnología de la organización de software malicioso y virus informáticos.

6. Definición y manejo de niveles de servicio y de operación para todos los procesos críticos de tecnología de información sobre la base de los requerimientos de los usuarios o clientes internos y externos de la entidad y a las capacidades tecnológicas.

7. Alineación de los servicios claves de tecnología de información con los requerimientos y las prioridades de la organización sustentados en la revisión, monitoreo y notificación de la efectividad y cumplimiento de dichos acuerdos.

8. Administración de los incidentes reportados, requerimientos de servicio y solicitudes de información y de cambios que demandan los usuarios, a través de mecanismos efectivos y oportunos como mesas de ayuda o de servicios, entre otros.

9. Mantenimiento de un repositorio de diagramas y configuraciones de hardware y software actualizado que garantice su integridad, disponibilidad y faciliten una rápida resolución de los problemas de producción.

10. Administración adecuada de la información, librerías de software, respaldos y recuperación de datos.

11. Incorporación de mecanismos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos, así como la protección y conservación de información utilizada para encriptación y autenticación.

410-13 Monitoreo y evaluación de los procesos y servicios

Es necesario establecer un marco de trabajo de monitoreo y definir el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad. La unidad de tecnología de información definirá sobre la base de las operaciones de la entidad, indicadores de desempeño y métricas del proceso para monitorear la gestión y tomar los correctivos que se requieran. La unidad de tecnología de información definirá y ejecutará procedimientos, mecanismos y la periodicidad para la medición, análisis y mejora del nivel de satisfacción de los clientes internos y externos por los servicios recibidos. La unidad de tecnología de información presentará informes periódicos de gestión a la alta dirección, para que ésta supervise el cumplimiento de los objetivos planteados y se identifiquen e implanten acciones correctivas y de mejoramiento del desempeño.

410-14 Sitio web, servicios de internet e intranet

Es responsabilidad de la unidad de tecnología de información elaborar las normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio WEB de la entidad, a base de las disposiciones legales y normativas y los requerimientos de los usuarios externos e internos.

La unidad de tecnología de información considerará el desarrollo de aplicaciones web y/o móviles que automaticen los procesos o trámites orientados al uso de instituciones y ciudadanos en general.

410-15 Capacitación informática

Las necesidades de capacitación serán identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constarán en un plan de capacitación informático, formulado conjuntamente con la unidad de talento humano. El plan estará orientado a los puestos de trabajo y a las necesidades de conocimiento específicas determinadas en la evaluación de desempeño e institucionales.

500 INFORMACIÓN Y COMUNICACIÓN

La máxima autoridad y los directivos de la entidad, deben identificar, capturar y comunicar información pertinente y con la oportunidad que facilite a las servidoras y servidores cumplir sus responsabilidades. El sistema de información y comunicación, está constituido por los métodos establecidos para registrar, procesar, resumir e informar sobre las operaciones técnicas, administrativas y financieras de una entidad.

La calidad de la información que brinda el sistema facilita a la máxima autoridad adoptar decisiones adecuadas que permitan controlar las actividades de la entidad y preparar información confiable. El sistema de información permite a la máxima autoridad evaluar los resultados de su gestión en la entidad versus los objetivos predefinidos, es decir, busca obtener información sobre su nivel de desempeño. La comunicación es la transmisión de información facilitando que las servidoras y servidores puedan cumplir sus responsabilidades de operación, información financiera y de cumplimiento. Los sistemas de información y comunicación que se diseñen e implanten deberán concordar con los planes estratégicos y operativos, debiendo ajustarse a sus características y necesidades y al ordenamiento jurídico vigente. La obtención de información interna y externa, facilita a la alta dirección preparar los informes necesarios en relación con los objetivos establecidos. El

suministro de información a los usuarios, con detalle suficiente y en el momento preciso, permitirá cumplir con sus responsabilidades de manera eficiente y eficaz.

1.2.4. Auditoría a la Seguridad Física

A pesar de que se invierte miles y en ocasiones millones de dólares en equipo de tecnología de punta para lograr los objetivos económicos que se propone una empresa, actualmente nos encontramos con que muchas organizaciones sufren de incidentes en donde se viola la Seguridad Física de sus instalaciones por terceros e inclusive por personal interno, esto posiblemente se debe, a que la Seguridad Física es en muchas ocasiones tomada como un elemento de "menor prioridad ", sea por iniciativa corporativa o por omisión.

Según PIATTINI, Mario y DEL PESO, Emilio; (2001). La Seguridad Física **"**garantiza la integridad de los activos humanos, lógicos y materiales de un CPD" (Pág. 182).

Según ECHENIQUE, José A.; (2002). Seguridad Física es "establecer políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de información, debido a contingencias como incendios, inundaciones, huelgas, disturbios, sabotaje, terremotos, huracanes etc., y continuar en un medio de emergencia hasta que sea restaurado al servicio completo" (pág. 219).

Las postulantes mencionan que la Seguridad Física es la verificación de todo elemento tangible que de una u otra manera interpreta o permita el correcto funcionamiento de la empresa y así garantizar la integridad de los activos humanos, lógicos y materiales. En definitiva la Seguridad Física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Es decir a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos

Para mejor comprensión del objetivo, instrumentos de evaluación, consideraciones y tipos de desastres de la Auditoría a la Seguridad Física se ha tomado en cuenta a PIATTINI, Mario y DEL PESO, Emilio; (2001), (182).

1.2.4.1. Objetivo Principal de Auditoría a la Seguridad Física

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

Los objetivos de la Seguridad Física se basan en prioridades con el siguiente orden:

1. Edificio

2. Instalaciones

3. Equipamiento y Telecomunicaciones

4. Datos y

5. Personas

1.2.4.2. Instrumentos de Evaluación en la Auditoría de la Seguridad Física

Antes

Grado de seguridad; es un conjunto de acciones utilizadas para evitar el fallo o, en su caso, aminorar las consecuencias que de él se puede derivar.

- ✓ **Entorno Físico**

    - Ubicación del Edificio
    - Ubicación del CPD dentro del edificio
    - Compartimentación
    - Elementos de construcción
    - Potencia eléctrica

- Sistemas contra incendios
- Control de acceso
- Selección del personal
- Seguridad de los medios
- Medidas de protección
- Duplicación de medios

Durante

Desastre; es cualquier evento que cuando ocurre tiene la capacidad de interrumpir el normal proceso de una empresa.

- ✓ **Plan de Contingencia**

  - Realizar un análisis de riesgos de sistemas críticos
  - Establecer un periodo crítico de recuperación
  - Realizar un análisis de aplicaciones críticas
  - Determinar las prioridades de los procesos por día
  - Establecer objetivos de recuperación
  - Designar un centro alternativo de procesos
  - Asegurar la capacidad de las comunicaciones
  - Asegurar la capacidad de los servicios de Back-up

Después

Los contratos de seguro, vienen a compensar las pérdidas, gastos o responsabilidades una vez corregido el fallo.

- ✓ **Seguros Existentes**

  - Centro de proceso y equipamiento
  - Reconstrucción de medio software
  - Gastos extras
  - Interrupción del negocio
  - Documentos y registros valiosos

- Errores y opiniones
- Cobertura de fidelidad
- Transporte de medios
- Contratos con proveedores y de mantenimiento

1.2.4.3. Consideraciones de la Auditoría a la Seguridad Física

En Cuanto al Lugar:

- Las paredes son de concreto sólido, excepto la parte de atrás y un costado que es de cancel.
- Existen ventanas amplias por donde entra la luz pero no los rayos del Sol.
- El techo está cubierto por plafón.
- La pintura de las paredes es de agua lavable.
- El Edificio cuenta con salidas de emergencia y extinguidores.

En Cuanto a la Instalación:

- Las mesas de trabajo cuentan con dos tomacorrientes cada uno regulados y polarizados con su respectiva conexión a tierra, diseñados especialmente para un solo equipo de cómputo.
- Las instalaciones eléctricas están ocultas, y las líneas están por encima del techo, al igual el cableado de datos estarán ocultos en Jack en cada mesa de trabajo.
- El centro de cómputo tendrá un centro de carga, este en caso de una variación eléctrica o apagones, evitará que se dañen los equipos y los mantendrá funcionando alrededor de las 24 horas los 7 días de la semana.

En Cuanto a los Equipos de Cómputo

- Las computadoras se conectarán a la red, mediante jumper, que irán de la tarjeta de red al Jack de terminación de la mesa.

- El gabinete que resguarda al Rack, cuenta con ventiladores los cuales sacarán el calor que generen los dispositivos dentro de éste.

- Los dispositivos del Rack, estarán conectados a un regulador UPS, el cual, en caso de un apagón, puede durar encendido 12 horas, de ésta manera evitará perder la información que en ése momento viaje por la red.

En Cuanto al Control de Accesos:

- Sólo podrán tener acceso al centro de cómputo, el personal autorizado.

- El edificio cuenta con vigilancia mediante guardias de seguridad, de día y de noche.

- El ITSC además implementará el sistema de vigilancia de circuito cerrado por medio de cámaras, esto para evitar robos dentro de la institución.

1.2.4.4. Tipos de Desastres en la Auditoría a la Seguridad Física

Entre los principales peligros que existen en un centro de datos nombraremos los siguientes:

Incendios: El centro de datos debe cumplir con normas de seguridad y debe tener sistemas contra incendios que eviten la propagación de incendios en caso de que sucedan, pero también debe permitir que en caso de que suceda un incendio la información pueda ser recuperada en su mayoría.

Inundaciones: Para evitar este inconveniente se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras. También sería conveniente estudiar el área para saber si en la misma

han sucedido inundaciones. En este caso se debe tomar las medidas preventivas necesarias.

Condiciones Climáticas: Esto no incluye solo a las condiciones climáticas, también incluye las condiciones internas del centro de cómputo ya que los equipos o Hardware necesitan de un ambiente ideal. Las temperaturas bajas o altas podría dañar los equipos por lo tanto sería conveniente contar con detectores de temperatura para estar pendiente de cambios que puedan afectar el centro de datos.

Señales de Radar: La influencia de las señales o rayos de radar sobre el funcionamiento de una computadora ha sido exhaustivamente estudiado desde hace varios años. Los resultados de las investigaciones más recientes son que las señales muy fuertes de radar pueden inferir en el procesamiento electrónico de la información, pero únicamente si la señal que alcanza el equipo es de 5Volts/Metro, o mayor. Ello podría ocurrir sólo si la antena respectiva fuera visible desde una ventana del centro de procesamiento respectivo y, en algún momento, estuviera apuntando directamente hacia dicha ventana. También el uso de telefonía celular dentro de los centros de datos en muchos casos no está permitido para evitar inconvenientes o problemas con los equipos.

Instalaciones Eléctricas: Es importante contar con buenas instalaciones eléctricas que estén instaladas cumpliendo con las normas establecidas para evitar fallas eléctricas, que puedan causar daños en los equipos, o podrían causar incendios.

Ergonomía: Es una disciplina que se ocupa de estudiar la forma en que interactúa el cuerpo humano con los artefactos y elementos que lo rodean, buscando que esa interacción sea lo menos agresiva y traumática posible.

También es necesario resguardar los equipos como ya que estos pueden ser utilizados para sacar información valiosa de la empresa, también para el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más

duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa. Los equipos de los que dispone la empresa también pueden ser utilizados para fraude por lo tanto es necesario dar a los usuarios accesos solo al material o la información necesaria.

Las investigadoras manifiestan que se evaluará las protecciones físicas de datos, programas, instalaciones, equipos, redes y soportes, y por supuesto habrá que considerar a las personas: que estén protegidas y existan medidas de evaluación, alarmas, salidas alternativas, así como que no estén expuestas a riesgos superiores a los considerados admisibles en la entidad e incluso en el sector. Las amenazas pueden ser muy diversas: sabotaje, vandalismo, terrorismo accidentes de distintos tipos, así como otros que afectan a las personas y puedan impactar el funcionamiento de los centros, tales como errores, negligencia, huelgas, epidemias o intoxicaciones.

Para mejor comprensión de la metodología y fases de la Auditoría Informática aplicables a la Seguridad Física se ha tomado en cuenta a RIVAS, Gonzalo; *Auditoría Informática*; Madrid; (1989), (Pág. 47-50).

1.2.4.5. Metodología y fases de la Auditoría Informática a la Seguridad Física

Existen algunas metodologías de Auditoría de Sistemas y todas dependen de lo que se pretenda revisar o analizar, pero como estándar, las cuatro fases básicas en un proceso de revisión son:

Fases de un proceso de Auditoría:

- ✓ Estudio preliminar
- ✓ Revisión y evaluación de controles y seguridades
- ✓ Examen detallado de áreas criticas
- ✓ Comunicación de resultados

1.2.4.5.1. Estudio Preliminar: En la ejecución de esta fase se copila y revisa documentos generales, políticas y objetivos de unidad, por otra parte en el cumplimiento del control interno puede conllevar a la suspensión de la auditoría; si el auditor considera que no existen mayores problemas o por el contrario observa justificativos para el desarrollo del ejercicio auditor, este tipo de metodología es un modelo basado en la LOAFYC.

- ✓ Designar Supervisor.
- ✓ Elaborar notificaciones de inicio de examen.
- ✓ Elaboración del programa de auditoría para esta fase.
- ✓ Visita a las dependencias del Área de Procesamiento de Datos (PAD).
- ✓ Entrevistas con los funcionarios.
- ✓ Obtención de informe general sobre políticas, objetivos, normas, procedimientos "Guía de Visita previa".
- ✓ Análisis de cumplimiento de objetivos establecidos para la creación del PAD.
- ✓ Elaboración de cedulas analíticas con información básica de la documentación obtenida, como manuales, instructivos, reglamentos, estándares, contratos, etc., aplicando su aplicabilidad en sus respectivas áreas.
- ✓ Evaluación preliminar del Control Interno a base de lista de chequeo, o cuestionarios de control interno.
- ✓ Informe de cumplimiento de la fase dirigido al Jefe de Auditoría.

1.2.4.5.2. Revisión y Evaluación de Controles y Seguridades: Consiste en la revisión de los diagramas de flujo de procesos, realización de pruebas de cumplimiento de las seguridades, revisión de aplicaciones de las áreas críticas,

revisión de procesos históricos (backups), revisión de documentación y archivos, entre otras actividades.

- ✓ Elaborar el Programa de Auditorías incluyendo procedimientos orientados hacia la revisión de la existencia de seguridad.
- ✓ Ejecución de los programas de Auditoría.
- ✓ Elaborar el informe de cumplimiento de la fase II

1.2.4.5.3. Examen Detallado de Áreas Críticas: Con las fases anteriores el auditor descubre las áreas críticas y sobre ellas hace un estudio y análisis profundo en los que definirá concretamente su grupo de trabajo y la distribución de carga del mismo, establecerá los motivos, objetivos, alcance recursos que usara, definirá la metodología de trabajo, la duración de la Auditoría, presentará el plan de trabajo y analizara detalladamente cada problema encontrado.

- ✓ Conformación de un equipo especializado de trabajo
- ✓ Con los resultados de las fases anteriores se procede a elaborar el plan específico de auditoría informática.
- ✓ Elaborar programas e ejecución de la fase III IV
- ✓ Realizar reuniones de trabajo con el personal involucrado en el examen.

1.2.4.5.4. Comunicación de Resultados: Se elaborará el borrador del informe a ser discutido con los ejecutivos de la empresa hasta llegar al informe definitivo, el cual presentará esquemáticamente en forma de matriz, cuadros o redacción simple y concisa que destaque los problemas encontrados, los efectos y las recomendaciones de la Auditoría.

- ✓ Cumplimiento de los programas establecidos en la fase anterior.
- ✓ Preparar un esquema de informe.

- ✓ En base a al esquema elaborar el informe a borrador, tomando como referencia de los hallazgos.

- ✓ Preparación del informe a borrador y la preparación de convocatoria para la lectura del informe a borrador.

- ✓ Elaboración del informe final de auditoría, incluyendo las observaciones y modificaciones planteadas en la conferencia final.

El informe debe contener lo siguiente:

- ✓ Motivos de la Auditoría
- ✓ Objetivos
- ✓ Alcance
- ✓ Estructura Orgánico-Funcional del área Informática
- ✓ Configuración del Hardware y Software instalado
- ✓ Control Interno
- ✓ Resultados de la Auditoría

Las postulantes consideran que la Auditoría Informática solo identifica el nivel de "exposición" por la falta de controles mientras el análisis de riesgos facilita la evaluación de los riesgos y recomienda acciones en base al costo-beneficio de la misma. Todas las metodologías existentes en Seguridad de Sistemas van encaminadas a establecer y mejorar un entramado de contramedidas que garanticen que la productividad de que las amenazas se materialicen en hechos sea lo más baja posible o al menos quede reducida de una forma razonable en costo-beneficio.

Para mejor comprensión de los Papeles de Trabajo se ha tomado en cuenta a ANDRADE, Ramiro; *Manual de la Auditoría de Gestión*; Ecuador; (2001), (Pág. 72,73).

1.2.5. Papeles de Trabajo

Se define como el conjunto de cédulas, documentos y medios magnéticos (tendencia a la Auditoría cero papeles) elaborados u obtenidos por el auditor gubernamental, producto de la aplicación de las técnicas, procedimientos y más prácticas de Auditoría, que sirve de evidencia del trabajo realizado y de los resultados de Auditoría revelados en el Informe.

Por lo tanto, constituye los registros y documentos y documentos mantenidos por el auditor de los procedimientos por el seguido, de las comprobaciones parciales que realizo a la información obtenida y de las conclusiones a las que arribo en relación con su examen; pueden incluir; programas de trabajo, análisis, anotaciones, documentos de la entidad o de tercero, cartas de confirmación y manifestaciones del clientes, extractos de documentos de la institución y planillas o comentarios preparados u obtenidos por el auditor.

Los propósitos principales de los Papeles de Trabajo son:

- ✓ Constituir el fundamento que dispone el auditor para preparar el Informe de Auditoría.
- ✓ Servirá de fuente para comprobar y explicar en detalle los comentarios, conclusiones y recomendaciones que se exponen en el Informe de Auditoría.
- ✓ Constituir la evidencia documental de trabajo realizado y de las decisiones tomadas. Todo esto de conformidad con las NAGA.
- ✓ Todo papel de trabajo debe reunir ciertas características, como las siguientes:
    - Prepararse en forma clara y precisa, utilizando referencias lógicas y un mínimo número de marcas.

- Su contenido incluirá tan solo los datos exigidos a juicio profesional del auditor.

- Deben elaborarse sin enmendaduras, asegurando la permanencia de la información.

- Se adoptaran las medidas oportunas para garantizar su custodia y confidencialidad, divulgándose las responsabilidades que podrían dar lugar por las desviaciones presentadas.

1.2.5.1. Los objetivos de los Papeles de Trabajo son los siguientes:

Principales:

- ✓ Respaldar el contenido del Informe preparado por el auditor
- ✓ Cumplir con las Normas de Auditoría emitidas por la Contraloría General

Secundarias:

- ✓ Sustentar el desarrollo de trabajo del auditor. El auditor ejecutara varias tareas personalmente o con la ayuda de sus operativos, las cuales requieren ciertas secuencias y orden para cumplir con las Normas Profesionales.
- ✓ Acumular evidencias, tanto de los procedimientos de Auditoría aplicados, como de las muestras seleccionadas, que permiten al auditor formarse una opinión del manejo financiero-administrativo de la entidad.
- ✓ Facilitar la supervisión y permitir que el trabajo ejecutado sea revisado por un tercero.
- ✓ Constituir un elemento importante para la programación de exámenes posteriores de la misma entidad o de otras similares.
- ✓ Informar a la entidad sobre las deficiencias observadas, sobre aspectos relativos a las actividades de control de los sistemas, de procedimientos contables entre otros.

- ✓ Sirve como defensa en posibles litigios o cargos en contra del auditor. Los Papeles de Trabajo, preparados con profesionales, sirven como evidencia del trabajo del auditor, posibilitando su utilización como elemento de juicio en acciones en su contra.

1.2.5.2. Custodia y Archivo

Los Papeles de Trabajo son de propiedad de las unidades de Auditoría de la Contraloría y las entidades públicas, las mismas que tienen la responsabilidad de la custodia en un archivo activo por el lapso de cinco años y en un archivo pasivo por hasta veinte y cinco años, únicamente puede ser exhibidos y entregados por requerimiento judicial.

Estos papeles de trabajo deben ser organizados y archivados en forma sistematizada, sea preparado legados, carpetas o archivos que son de dos clases:

Archivo Permanente o Continuo.- Este archivo permanente contiene información de interés o utilidad para más de una Auditoría o necesarias para Auditorías subsiguientes.

- ✓ La primera hoja de este archivo necesariamente debe ser de índice, el mismo que indica el contenido del legajo.
- ✓ La finalidad del archivo permanente se puede resumir en los puntos siguientes:
- ✓ Recordar al auditor las operaciones, actividades o hechos que tiene vigencia en un periodo de varios años.
- ✓ Proporcionar a los auditores nuevos, una fuente de información de la Auditorías realizadas.
- ✓ Conservar Papeles de Trabajo que serán utilizados durante varios años y que no requiere ser preparados años tras años, ya que no se ha operado ningún cambio.

- ✓ La mayor parte de información se obtiene en la primera Auditoría, pero como se indicó su utilización es en esta y futuras Auditorías.

Archivo Corriente.- En este archivo corriente se guardan los Papeles de Trabajo relacionados con la Auditoría específica de un período. La cantidad de legajos o carpetas que forman parte de este archivo de un período dado varia de una Auditoría a otra y aun tratándose de la misma entidad auditada. Este Archivo a su vez se divide en dos legajos o carpetas, una con información general y la otra con documentación especifica por componentes.

1.2.5.3. Índices y Referencias

Es necesario la anotación de índices en los Papeles de Trabajo ya sea en el curso o al concluirse la Auditoría, para lo cual primeramente se debe definir los códigos a emplearse que deben ser iguales a los utilizados en los archivos y su determinación debe considerase la clase de archivo y los tipos de Papeles de Trabajo.

Es importante también que todos los Papeles de Trabajo contengan referencias cruzadas cuando están relacionados entre sí, esto se realiza con el propósito de mostrar en forma objetiva como se encuentra ligados o relacionados entre sí los diferentes Papeles de Trabajo.

La codificación de índices y referencias en los Papeles de Trabajo pueden ser de tres formas:

- Alfabética
- Numérica
- Alfanumérica

El criterio anteriormente expuesto fue para el archivo permanente índices numéricos y para el archivo corriente índices alfabéticos y alfanuméricos.

1.2.5.4. Marcas de Auditoría

Las marcas de Auditoría, conocida también como: claves de Auditoría o tildes, son signos particulares y distintivos que hace el auditor para señalar el tipo de trabajo realizado de manera que el alcance del trabajo quede perfectamente establecido. Estas marcas permite conocer además, cuáles partidas fueron objeto de la aplicación de los procedimientos de Auditoría y cuáles son:

Existen dos tipos de marcar, las de significado uniforme y que para su compresión requiere que junto al símbolo vaya una leyenda de su significado.

Las marcas a igual de los índices y referencias ya indicadas, preferentemente debe ser escrita con lápiz de color rojo, ya que se encuentra generalizado al igual que los Papeles de Trabajo elaborados por el auditor usualmente son hechos con lápiz de papel.

A continuación propongamos las marcas estándares que pueden utilizarse y que se encuentran relacionadas con las técnicas y otras prácticas que contienen los procedimientos de Auditoría.

¢ Comentario referencia a controles manuales.

∫ Comentario referente a formularios

@ Comentario referente a controles automáticos

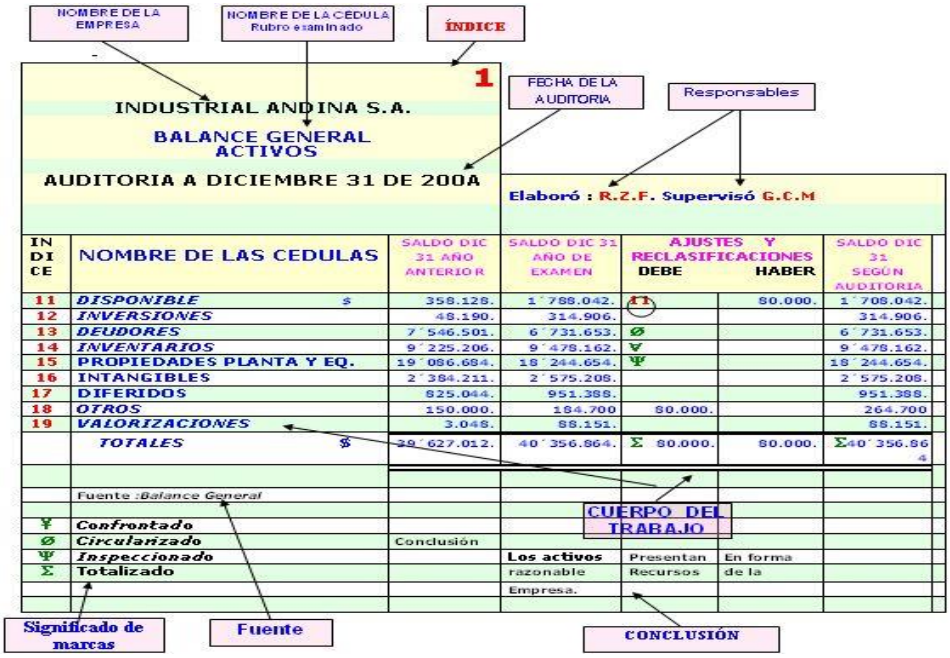
C Circularizados

Ø Inspeccionado

Las investigadoras manifiestan que los Papeles de Trabajo sirven para dejar constancia escrita del trabajo realizado por el auditor, además recogen las conclusiones a las que llega el auditor como resultado de su trabajo, los Papeles de Trabajo tienen que confeccionarse, organizarse y clasificarse con la suficiente

sencillez y claridad como para que puedan ser comprendidos sin ningún tipo de aclaración o explicación adicional, Los mismos que tienen valor probatorio en caso de juicio, por lo que pueden ser útiles para un auditor acusado de fraude o negligencia. Conforme a lo dispuesto en la Ley de Auditoría, los papeles de Trabajo son propiedad del auditor, el cual debe conservarlos por un período de cinco años, aunque la información que contienen es totalmente confidencial, y nadie puede utilizarla sin el consentimiento de la compañía auditada, existen, no obstante, ciertas excepciones al secreto profesional, como son: por mandato judicial, quienes estén autorizados por la ley, en el ejercicio del control técnico del auditor.

GRÁFICO 2. EJEMPLO DE PAPELES DE TRABAJO



Fuente: *http://fccea.unicauca.edu.co/old/tgarf/tgarfse130.html*
Elaborado por: Las investigadoras

CAPÍTULO II

MARCO INVESTIGATIVO

2. Breve Caracterización del Objeto de Estudio

2.1. Reseña histórica

La Ley Orgánica de la Policía Nacional en su Art. 53 del año 1998, crea la Dirección Nacional de Comunicaciones, y mediante RESOLUCIÓN No. 2000-353-CG-PN del 3 de Octubre del 2000, aprueba y expide el Reglamento Orgánico - Funcional de la Dirección Nacional de Comunicaciones de la Policía Nacional.

En el año 2000 la Dirección Nacional de Comunicaciones funcionaba en el Rancho San Vicente en las oficinas pertenecientes al Club de Oficiales de la Policía Nacional junto a la Escuela de Especialización y Perfeccionamiento de Oficiales, bajo una estructura orgánica muy básica.

En el año 2001, posterior a la aprobación del Reglamento Orgánico - Funcional, la Dirección Nacional de Comunicaciones arrienda un edificio en las Calles José Ortón y Paúl Rivet, para el funcionamiento técnico administrativo de conforme a la nueva estructura organizacional aprobada.

En el año 2002 el señor Crnl. Ing. Carlos Grijalva Director Nacional de Comunicaciones, realiza las gestiones respectivas ante el Ministerio de Finanzas y consigue en calidad de comodato por 50 años una infraestructura física ubicada en el sector la Gasca, sitio estratégico desde el punto de vista técnico.

Se realiza las adecuaciones y mantenimiento de la infraestructura física de la edificación otorgada en comodato

Desde el año 2003 hasta la presente fecha el Centro de Datos de la Dirección Nacional de Telecomunicaciones, funciona en las calles Rither Oe 9-141 y Diego Zorrila sector La Gasca.

2.1.1. Ubicación geográfica

Calles Rither Oe 9-141 y Diego Zorrila sector La Gasca.

2.1.2. Misión

Liderar la prestación de los servicios de telecomunicaciones e informática, a través de una constante preparación del talento humano y la utilización de las tecnologías adecuadas que garantice la eficiencia y eficacia en apoyo a la labor institucional y a la comunidad.

2.1.3. Visión

La Dirección Nacional de Telecomunicaciones e Informática, será reconocida por el desarrollo e incorporación de tecnologías de información y comunicación mediante una capacitación permanente, investigación continua, una activa vinculación e innovación tecnológica con estándares de calidad que contribuyan a garantizar la seguridad y operatividad de los servicios informáticos y de comunicación.

2.1.4. Objetivos organizacionales

Objetivo General

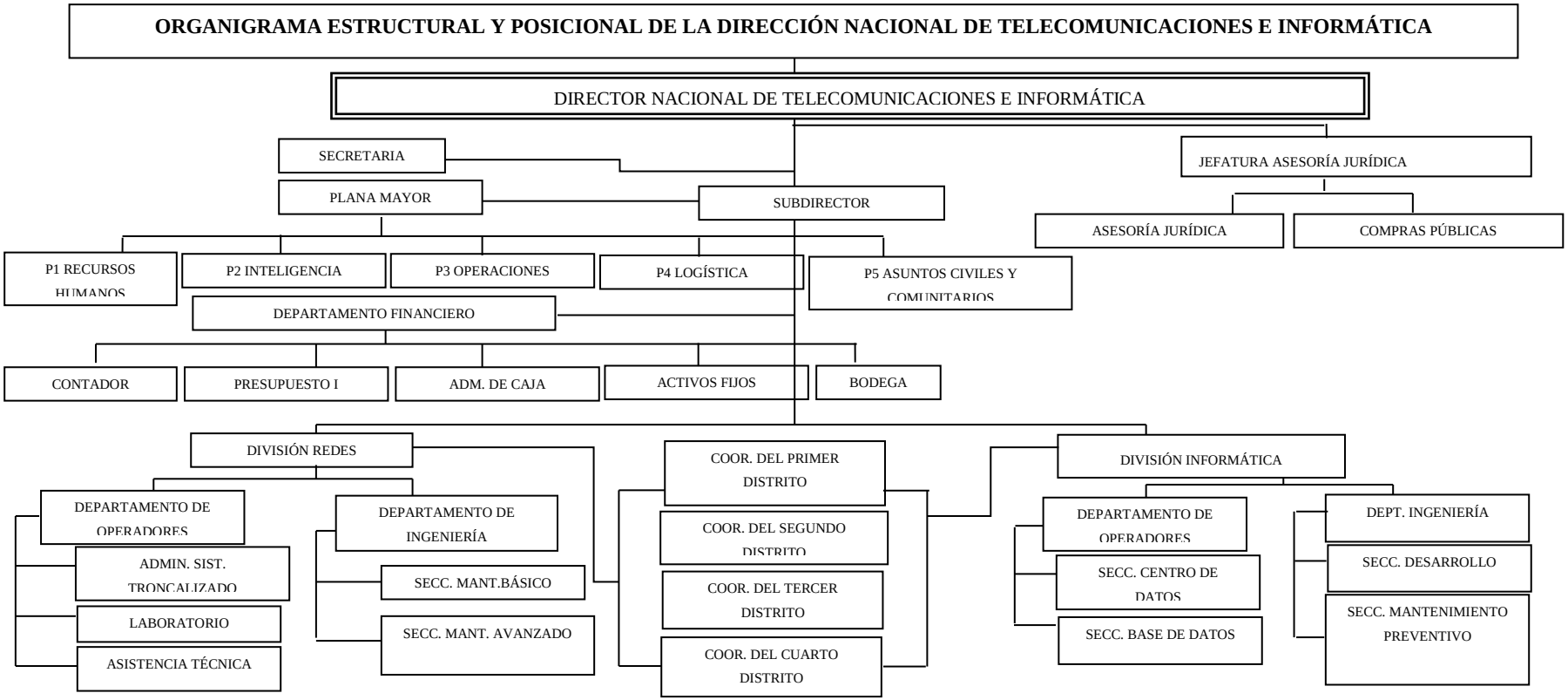
Desarrollar las funciones de comunicaciones e informática, para apoyar todas las labores de la Policía Nacional a fin de optimizar la gestión institucional

Objetivos Específicos

- ✓ Lograr y mantener el más alto grado de calidad en los servicios de telecomunicaciones e informática de la Policía Nacional.
- ✓ Procurar la excelencia administrativa de la infraestructura existente en la Policía Nacional en materia de telecomunicaciones e informática.
- ✓ Estandarizar la infraestructura tecnológica.
- ✓ Centralizar las decisiones tecnológicas y descentralizar las acciones operacionales.
- ✓ Promover la modernización constante y del desarrollo continuo en los servicios de comunicaciones e informática.
- ✓ Fortalecer la participación Policial con la comunidad a través del asesoramiento en materia de comunicaciones e informática.

2.1.5. Estructura organizacional

GRÁFICO 3. ORGANIGRAMA D.N.T.I.



Fuente: Dirección Nacional de Telecomunicaciones e Informática
Elaborado por: Las investigadoras

2.1.6. Funciones principales de la División Redes

- Proponer alternativas de última tecnología, a través del diseño y ejecución de proyectos tecnológicos, manteniendo los estándares de calidad y seguridad, para mejorar los procesos administrativos y operativos en la institución.

- Administrar y mantener operativo los diferentes sistemas de comunicaciones, disponiendo del recurso humano y los medios técnicos necesarios.

- Brindar el mantenimiento preventivo y correctivo del equipamiento tecnológico y el asesoramiento y soporte técnico inmediato a las Unidades y Servicios Policiales a nivel nacional.

- Supervisar el correcto uso del espectro radioeléctrico en las bandas asignadas a la Policía Nacional a nivel nacional.

2.2. Diagnostico situacional de la institución

2.2.1. Análisis Macroambiente

Son aquellos factores que las instituciones no pueden controlar y un cambio en uno de ellos ocasionará serias consecuencias; además está compuesto por las fuerzas que dan forma a las oportunidades o presentan una amenaza para la institución.

- **Factor Tecnológico**

La tecnología en el mundo actual es un factor determinante para el desarrollo de un país como para el desarrollo de las instituciones, esta permite la reducción de costos. La evolución tecnológica mundial constituye una **OPORTUNIDAD** para la División Redes debido a que la ha obligado a mantenerse a la par o emprender planes con el fin de explotar de mejor manera la tecnología existente. Pero al igual que mejora la tecnología también aumenta las **amenazas** cibernéticas por medio de

creación de virus y otras **AMENAZAS** que impiden el adecuado manejo de la información.

- **Factor Político**

Supone como su figura el sistema y el poder político en la sociedad, poderes políticos, partidos políticos, clima social.

La estabilidad política que vive el país se constituye en una **OPORTUNIDAD** que tiene la División Redes para seguir con sus planes de crecimiento e inversión y mantenimiento de la visión a mediano y largo plazo.

- **Factor Legal**

Implica la consideración del sistema legal jurídico administrativo y fiscal jurisdicción, legislación específica sobre las organizaciones.

En esta institución se rigen bajo a la Ley orgánica de servicio público, Ley orgánica de la Policía Nacional, Reglamento de disciplina de la Policía, Código de ética profesional de la Policía Nacional y Código penal de la Policía Nacional; mismas que con cumplidas a cabalidad, demostrando así la buena atención tanto a usuarios internos como externos. Siendo para la institución una **OPORTUNIDAD**.

- **Factor Económico**

Recaudación tributaria

La recaudación efectiva (sin considerar devoluciones de impuestos) en el periodo Enero–Diciembre 2011 se ubicó en US$9.561 millones de dólares, con un crecimiento nominal de 14.4% frente al mismo período del año anterior. El monto recaudado presenta un cumplimiento del 109,8% frente a la meta proporcional prevista para el período.

La mayor recaudación de tributos es una **OPORTUNIDAD** para la Dirección Nacional de Telecomunicaciones e Informática por ende beneficia a la División

Redes, pues obliga a que todas las empresas privadas transparenten sus ingresos y asegura el presupuesto de las Empresas Públicas.

- **Factor Geográfico**

Comprende la naturaleza, calidad y cantidad y disponibilidad de recursos naturales, condiciones geográficas y climáticas.

La institución se encuentra ubicada en la ciudad de Quito, sector la Gasca perteneciente a la región sierra, la significa una **OPORTUNIDAD** debido a que se encuentra en la centro de país, pero también es una **AMENAZA** debido a los cambios climáticos los cuales son tendientes a generar descargas eléctricas ocasionando averías en los equipos.

2.2.2. Análisis Microambiente

Se debe evaluar y examinar el ambiente interno y lo que respecta a los recursos, lo mismo que sus fortalezas y debilidades en investigación, desarrollo, operación de los servicios.

Para lo cual los Factores internos positivos son fuerzas impulsadoras que contribuyen positivamente a la empresa. Recursos que se pueden controlar capacidades y habilidades que se poseen, actividades que se desarrollan positivamente y factores internos negativos son fuerzas obstaculizantes o problemas que impiden el adecuado desempeño. Recursos de los que carece, habilidades que no se poseen, actividades que no desarrollan positivamente.

- **Talento Humano**

La División Redes cuenta con 10 personas capacitadas en cada área, con titulo de tercer nivel, que se encuentran distribuidos de la siente manera: tres técnicos en la sección ingeniería, tres técnicos en la sección operaciones y cuatro administradores del sistema troncalizado posen títulos de Ing. Eléctrica, Electrónica sistemas computacionales la cual representa una **FORTALEZA.**

- **Infraestructura**

La infraestructura de la División Redes se encuentra en mal estado físico debido a la falta de mantenimiento del edificio División Redes la cual representa una **DEBILIDAD** para la institución.

- **Organización**

La División Redes por ser parte de la Policía Nacional está sometida a cambios de los mandos policiales ya que con frecuencia se integran nuevos jefes policiales que algunas veces desconocen de la labor que la institución realiza, la cual representa una **DEBILIDAD**.

- **Tecnología**

La institución cuenta con equipos cómputo y de comunicación de última tecnología que fue adquirido en el presente año por lo cual representa una **FORTALEZA** para la institución.

- **Cliente**

La institución presta servicios de comunicación de radio, servicio de correo electrónico y base de datos de la Policía Nacional siendo una **FORTALEZA** el buen trato que brinda el personal a sus usuarios.

- **Proveedores**

La Dirección Nacional de Telecomunicaciones e Informática por ser una institución del sector público realiza sus compras por medio del sistema de compras públicas la cual representa una **FORTALEZA**, debido a la variedad de ofertas que recibe.

2.2.3. Análisis FODA

Tanto las fortalezas como las debilidades son internas de la organización, por lo que es posible actuar directamente sobre ellas. En cambio las oportunidades y las amenazas son externas, por lo que en general resulta muy difícil poder

modificarlas y ejercer control sobre ellas. Es importante determinar cada uno de estos factores para que la administración pueda tomar decisiones acertadas que ayuden al mejoramiento y desarrollo de la empresa. Para la elaboración del análisis FODA se lo ha realizado por medio de la aplicación de entrevistas, encuestas y por la observación directa ya que se ha palpado personalmente en parte la situación en la que se encuentra actualmente, para lo cual se detalla a continuación:

TABLA 1. ANÁLISIS FODA

FORTALEZAS	DEBILIDADES
✓ Personal capacitado ✓ Trabajo en equipo. ✓ Tecnología de punta ✓ Buen trato al usuario interno y externo ✓ Servicio de internet adecuado	✓ Cambio de mandos policiales. ✓ Infraestructura inadecuada. ✓ Carencia de un Plan Estratégico ✓ Falta de control de los Activos Fijos ✓ Carencia de un Plan de Contingencia ✓ Falta de coordinación y toma de decisiones.
OPORTUNIDADES	**AMENAZAS**
✓ Desarrollo Tecnológico ✓ Apoyo económico a través del Ministerio del Finanzas. ✓ Convenios y alianzas estratégicas con el Sector Público y Privado a nivel nacional e internacional. (CNT y Motorola). ✓ Buena ubicación geográfica	✓ Inestabilidad Política ✓ Virus ✓ Pérdida de información ✓ Cortes de energía eléctrica por condiciones climáticas.

Fuente: Dirección Nacional de Telecomunicaciones e Informática
Elaborado por: Las Tesistas

2.3. Diseño Metodológico

2.3.1. Tipo de Investigación

Investigación bibliográfica

En esta investigación se recabó la información necesaria para documentar los conceptos teóricos en base a libros y publicaciones en internet de expertos en el

área de la seguridad informática, enfocándonos principalmente en la seguridad física para garantizar la seguridad del centro de datos. Los datos recopilados ayudaron a estructurar el marco teórico para posteriormente realizar la investigación de campo.

Investigación de campo

Con esta investigación se consigue valorar la necesidad real que existe para implementar la Tesis; ya que, se elaboró una encuesta dirigida al personal técnico y una entrevista tanto al Director Nacional Coronel Jaime Jara como al Jefe de la División Redes Mayor Giovanni Naranjo. Permitiendo aclarar la necesidad de la aplicación de una Auditoria Informática a la Seguridad Física.

Investigación aplicada

Para la aplicación de la Auditoria Informática a la Seguridad Física se utilizó todos los conocimientos teóricos y prácticos. Para conseguir el resultado esperado se realizó planes y programas en los que se incluyen todas las tareas a efectuarse durante todo el proceso de Auditoria, todo el trabajo se refleja en un informe final que se presenta al Jefe de la División Redes de la Dirección Nacional de Telecomunicaciones e Informática de la Policía Nacional.

2.3.2. Metodología

La metodología que se utiliza es la no experimental, ya que la información es observada tal y como ocurre, sin manipular las variables. Para el trabajo de campo las tesistas aplicaron algunas encuestas e instrumentos de investigaciones, para que basados en ellas se pueda obtener mejor información para la aplicación de la Propuesta.

2.3.3. Métodos de Investigación

Método Deductivo.- Es un proceso reflexivo, sistemático, parte de un principio general ya conocido para relacionar en consecuencias particulares, expresando de una forma más sencilla, la deducción consiste en partir de una teoría en general para aplicar hechos o fenómenos particulares.

La aplicación de este método se utilizó para el diseño del marco teórico de la tesis, con la finalidad de identificar los principales hechos para ir describiéndolos, además ayudará a presentar alternativas o mejoras a la institución.

Método Inductivo.- Es un método en el cual se puede obtener conclusiones generales de indicios particulares.

Este método nos ayudó a obtener un conocimiento global del sistema de gestión de la calidad aplicando la evaluación del control interno y así concluye con el informe y recomendaciones que la empresa debe seguir para mejorar las deficiencias obtenidas

Método Analítico.- Es un método que implica el análisis del problema, ya que consiste en la separación de un todo en sus partes o en sus elementos constitutivos.

Este método se aplicó a través de la verificación de los procedimientos analíticos en la planificación del trabajo esto ayudo al auditor en la determinación de la naturaleza, oportunidad y alcance de otros procedimientos de Auditoría.

2.3.4. Técnicas de Investigación

2.3.4.1. Observación.- Es una técnica que permitió obtener un conocimiento acerca del comportamiento del objeto de la investigación, tal como este se da en la realidad, además es una manera de obtener información directa e inmediata sobre el fenómeno u objeto investigativo.

En esta técnica se ve reflejada un formulario de visita previa, donde se puede examinar de manera general cada una de las fortalezas o debilidades que posee la institución a ser evaluada

2.3.4.2. Entrevista.- Es un dialogo que tiene como finalidad obtener información sobre los fenómenos investigados y comprobar así sus teorías, es decir se trata de una situación en la que una persona se somete a las preguntas realizadas por otra.

La entrevista es una técnica de investigación que permitió obtener información de gran importancia en base a preguntas, la misma que se aplicó al Director Nacional

Coronel Jaime Jara y al Mayor Giovanni Naranjo, los cuales contribuyeron con su experiencia laboral.

2.3.4.3. Encuesta.- La encuesta es una técnica destinada a obtener datos de varias personas cuyas opiniones impersonales interesan al investigador.

Se utilizó esta técnica para obtener información, la misma que se basa en preguntas que deben son contestadas por el personal técnico de la institución. Dichas preguntas son formuladas de tal forma que la respuesta afirmativa indican un punto óptimo en la estructura de Control Interno y que una respuesta negativa indica una debilidad y un aspecto no muy confiable y así se pudo determinar las áreas más críticas.

2.4. Unidad de Estudio

La población para la presente investigación en la División de Redes de la Dirección Nacional de Telecomunicaciones e Informática de la Policía Nacional, esta distribuido de la siguiente manera:

TABLA 2. POBLACIÓN O UNIVERSO

DESCRIPCIÓN	CANTIDAD
Director D.N.T.I. Policía Nacional	1
Jefes División Redes D.N.T.I. Policía Nacional	2
Técnicos División Redes D.N.T.I. Policía Nacional	10
TOTAL	**13**

Fuente: Dirección Nacional de Telecomunicaciones e Informática
Elaborado por: Las investigadoras

2.5. Preguntas Científicas

¿Qué contenidos teóricos permitirán el desarrollo de una Auditoría que evalúe el desempeño de las seguridades de hardware en la División Redes de la DNTI?

Para la aplicación de la Auditoria se realizó una búsqueda de los temas relacionados con la investigación. A demás la lectura de documentos impresos y

electrónicos referentes a Auditoria Informática, y Auditorías Físicas; ha permitido evaluar adecuadamente el desempeño de cada una de las seguridades que posee el Centro de Datos de la División Redes.

¿Cuáles son los principales problemas que presenta la División Redes de la DNTI, al no contar con un adecuado control de los manuales y planes de seguridades de los sistemas de información?

Al no contar con un adecuado manejo de la documentación con respecto a manuales, políticas o planes estratégicos, sus problemas son muchos; principalmente uno de ellos es la perdida de información, esto debido a la falta de un plan de contingencia el mismo que sirve de gran ayuda en casos de desastres ocasionados por la naturaleza o por el hombre mismo.

¿Qué características importantes debería tener la Auditoría Informática a la Seguridad Física, para mejorar el desempeño de los sistemas de información y del personal de la División Redes de la DNTI?

Una de las características es que debe ser evaluada por una persona que tengas conocimientos generales en el área informática y de auditoría para que por medio de la aplicación de una metodología adecuada y acorde a las necesidades se logre establecer políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de información, ocasionados por diversos desastres naturales como humanos y por ende salvaguardar la seguridad de los equipos informáticos como la del talento humano de la institución.

2.6. Operacionalización de las Variables

TABLA 3. OPERACIONALIZACIÓN DE LAS VARIABLES

PREGUNTAS CIENTÍFICAS	VARIABLES	DIMENSIÓN	INDICADORES	INSTRUMENTOS
¿Qué contenidos teóricos permitirán el desarrollo de una Auditoría que evalúe el desempeño de las seguridades de hardware en la División Redes de la DNTI?	Auditoría Informática	• Procedimiento de los controles físicos.	• Normativas • Reglamento de Disciplina de la Policía • Ley Orgánica de la Policía Nacional • Código de Ética Profesional de la Policía Nacional	• Ficha de Observación • Encuesta • Guía de Entrevista
¿Cuáles son los principales problemas que presenta la División Redes de la DNTI, al no contar con un adecuado control de los manuales y planes de seguridades de los sistemas de información?	Mejorar el desempeño de los sistemas de información y del personal	• Proceso administrativo de la seguridad • Plan de contingencia • Análisis FODA	• Planificación de actividades • Seguimiento a las actividades • Fortalezas, Debilidades, Oportunidades, Amenazas.	
¿Qué características importantes debería tener la Auditoría Informática a la Seguridad Física, para mejorar el desempeño de los sistemas de información y del personal de la División Redes de la DNTI?	Auditoría Informática a la Seguridad Física	• Control Interno • Metodología de la Auditoría Informática	• Matriz de riesgos • Evaluación del riesgo • Estudio Preliminar • Revisión y evaluación de controles y seguridades. • Examen detallado de las áreas críticas. • Informe final	

Fuente: Anteproyecto de tesis
Elaborado por: Las Tesistas

2.7. Entrevista al Coronel Jaime Jara Director Nacional de Telecomunicaciones e Informática de la P.N.

OBJETIVO: Obtener información fundamental para evaluar los controles organizacionales, a través los documentos, manuales y la estructura jerárquica dentro de la Dirección Nacional de Telecomunicaciones e informática de la Policía Nacional.

1.- ¿Se ha realizado algún tipo de Auditoría en la Dirección Nacional de Telecomunicaciones e Informática?

Si como por ejemplo una Auditoría a los Activos Fijos solicitada por la Comandancia General y una Auditoría de Gestión solicitada por la D.N.T.I, misma que no cumplió con nuestras expectativas.

2.- ¿La Dirección Nacional de Telecomunicaciones e Informática cuenta con una planificación estratégica?

Sí, pero no se encuentra bien estructurada.

3.- ¿Qué estrategias se han establecido para el cumplimiento de los objetivos de la Dirección Nacional de Telecomunicaciones e Informática?

Entre las estrategias tenemos las siguientes con mayor relevancia:

- ✓ Calidad y servicio en el asesoramiento tecnológico a la policía.
- ✓ Actualización tecnológica.
- ✓ Servicio personalizado a la comunidad policial..
- ✓ Mejoramiento continuo del servicio a los clientes (policías)
- ✓ Capacitación al personal y usuarios.

4.- ¿Con qué tipos de manuales cuenta la Dirección Nacional de Telecomunicaciones e Informática?

Únicamente con los Manuales de Procedimientos del uso de Equipos de Comunicación.

5.- Mencione ¿cuáles son las políticas institucionales que tiene la D.N.T.I.?

- ✓ Proteger la confidencialidad, seguridad e integridad de la información de nuestros clientes (policías), mediante medidas de seguridad integral.
- ✓ Respetar en todo momento los compromisos con el cliente, los compañeros y proveedores.
- ✓ Liderar el talento humano policial para alcanzar un alto rendimiento de forma continua, logrando ser efectivos en el cumplimiento de la misión institucional de "Atender la seguridad ciudadana y el orden público, y proteger el libre ejercicio de los derechos y la seguridad de las personas dentro del territorio nacional", etc.

6.- ¿Se encuentran establecidas en algún documento las funciones del personal?

No, ya que únicamente se lo realiza a través de órdenes o memorándums, para la asignación de tareas.

GRACIAS POR SU COLABORACIÓN

2.8. Análisis de los resultados de la entrevista aplicada al Coronel Jaime Jara Director Nacional

Una vez efectuado la respectiva entrevista al Director Nacional de Telecomunicaciones e informática se ha logrado resaltar que en esta institución se ha realizado dos Auditorías como es el caso de una Auditoría Financiera a pedido de la Comandancia General y una Auditoría de Gestión con el propósito de que les ayuden a elaborar los Manuales de Funciones y Procedimientos, situación que esta el momento no se ha dado cumplimiento, generando así que la D.N.T.I.P.N., no cuenta con un Manual de Funciones que soporte la ejecución de cada una de las funciones del personal, mismo que conlleva a la incomodidad laboral.

Además como es una institución que pertenece a la Policía Nacional están regidos a la Ley Orgánica de Policía, por ende se basan en las ordenes encomendadas por los superiores sean están de forma oral o escrita (memorándums), de la misma manera se ha constatado el cumplimiento de las estrategias encaminadas al logro de los objetivos institucionales como es el caso del personal capacitado, el mejoramiento de nuevas tecnologías, calidad y servicio en el asesoramiento tecnológico, etc., lo cual ocasiona el fortalecimiento de la institución.

2.9. Entrevista al Jefe de la División Redes Mayor Giovanni Naranjo

OBJETIVO: Recolectar información fundamental para evaluar los controles y seguridades físicas, lo cual facilitará la identificación de las debilidades o fortalezas de la División Redes de la Dirección Nacional de Telecomunicaciones e Informática.

1.- ¿Quiénes están autorizados al acceso a los archivos y programas en la División Redes de la Dirección Nacional de Telecomunicaciones e Informática?

Únicamente están autorizados a los archivos el Jefe de la División Redes conjuntamente con su Secretaria, mientras que a los programas los Administradores del Sistema.

2.- ¿Cuál es la persona responsable de la seguridad dentro del área de División Redes de la Dirección Nacional de Telecomunicaciones e Informática?

Cuentan con el Servicio de Guardianía Policial, mismos que lo ejercen dos miembros policiales en tres turnos rotativos y pertenecen a la institución.

3.- ¿Qué medidas de seguridad tiene establecido el departamento de la División Redes de la Dirección Nacional de Telecomunicaciones e Informática de la Policía Nacional?

- ✓ Disponibilidad de sensores de humo; alarmas, mangueras contra incendios; extintores; cámaras de vigilancias las 24h00 del día.

- ✓ Registro de ingresos y salidas tanto del personal como de personas ajenas a la institución efectuado por los guardias policiales, dicho registro se lo realiza en un libro.
- ✓ Control de acceso por medio de biométrico

4.- ¿La división Redes cuenta con algún Plan de Contingencia ante cualquier tipo de desastre?

En la actualidad no se cuenta con un Plan de Contingencia.

5.- ¿Qué políticas de seguridad física tiene la a División Redes?

No se cuenta con políticas de Seguridad Física.

6.- ¿Se ha dado cumplimiento a todos los proyectos programados para este año?

Si, por ejemplo la implementación de la Red Troncalizado Nacional, en la que incluye cobertura del Sistema, transmisión de datos, ubicación con GPS, programación a través del aire (OTAP), sistema de encriptación vía aire (OTAR).

7.- ¿Qué medidas de control se tiene para la protección de los equipos?

- ✓ Monitoreo del funcionamiento de los equipos las 24 horas del día, con un Técnico y un Administrador de turno.
- ✓ Los Usuarios de los Equipos Terminales de Comunicación, alertan cualquier anomalía en el funcionamiento de los mismos.

GRACIAS POR SU COLABORACIÓN

2.10. Análisis de los resultados de la entrevista aplicada al Jefe de la División Redes Mayor Giovanni Naranjo

Una vez realizada la entrevista al Jefe de la División Redes a mencionado que una de las principales funciones de este departamento es "administrar y mantener operativo los diferentes sistemas de comunicaciones, disponiendo del recurso humano y los medios técnicos necesarios", esto se logra a través de un adecuado control a la seguridad misma que está a cargo del servicio de guardianía policial, ya que llevan un registro de entrada y salida tanto del personal como de personas particulares, también cuenta con un biométrico para el ingreso y salida del personal, además la institución cuenta con sensores de humo, alarmas contra incendios, extintores, cámaras de vigilancia las 24 horas del día como una medida de seguridad ante cualquier desastre, hay que resaltar que este departamento no cuenta con un Plan de Contingencia ante cualquier desastre pese a la gran cantidad de información y equipos que tiene por salvaguardar el cual representa una gran debilidad institucional.

A si mismo se menciona que los únicos que tienen acceso a los archivos de este departamento son el Jefe y su Secretaria, mientras que a los programas como ejemplo el Docpol los Administradores del Sistema; uno de los proyectos cumplidos es la implementación de la Red Troncalizado a nivel Nacional, misma que incluye la transmisión de datos, ubicación con GPS, programaciones a través del aire, Sistema de Encripción vía aire mismo que beneficiará no solo a la Policía sino a toda la colectividad.

2.11. Análisis e interpretación de los resultados de las encuestas aplicadas al personal de la División Redes de la Dirección Nacional de Telecomunicaciones e Informática de la P.N.

OBJETIVO: Obtener información fundamental para evaluar los controles y seguridades dentro de la División Redes de la Dirección Nacional de Telecomunicaciones e informática de la Policía Nacional.

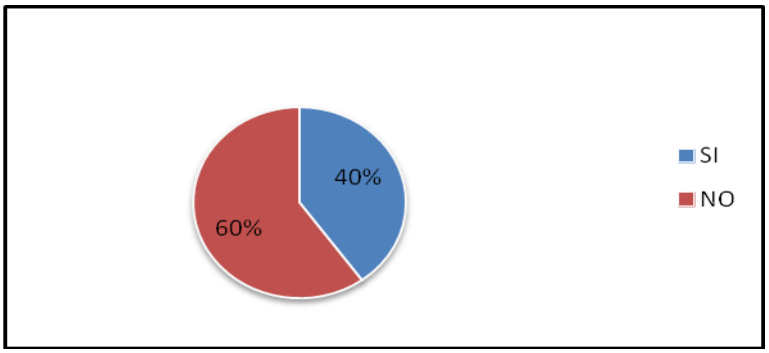
1.- ¿Se han adoptado medidas de seguridad en la División Redes?

TABLA 4. SEGURIDAD EN LA DIVISIÓN REDES

ALTERNATIVAS	FRECUENCIA	PORCENTAJES
SI	4	40%
NO	6	60%
TOTAL	**10**	**100%**

Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

GRÁFICO 4. SEGURIDAD EN LA DIVISIÓN REDES



Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

ANÁLISIS E INTERPRETACIÓN

De las 10 personas encuestadas en la División Redes 6 empleados que representan al 60% manifiestan que se han adoptado medidas de seguridad en la División Redes; mientras que 4 de los empleados que representan al 40% revelan que la institución no cuenta con una buena seguridad dentro de la división redes. Por lo tanto es necesario que los directivos o Jefes departamentales den a conocer a todo el personal sobre las diferentes medidas de seguridad que poseen en todos los departamentos.

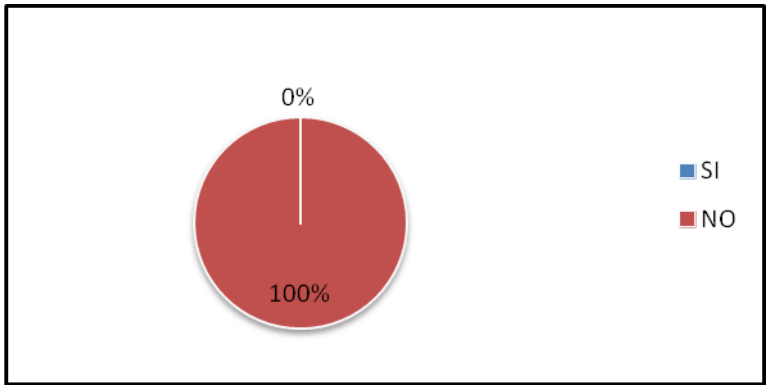
2.- ¿Existe salida de emergencia?

TABLA 5. SALIDA DE EMERGENCIA

ALTERNATIVAS	FRECUENCIA	PORCENTAJES
SI	0	0%
NO	10	100%
TOTAL	**10**	**100%**

Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

GRÁFICO 5. SALIDA DE EMERGENCIA



Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

ANÁLISIS E INTERPRETACIÓN

De las 10 personas encuestadas en la División Redes los 10 empleados que representa el 100% expresaron que la División Redes y en general toda la Dirección de Telecomunicaciones e Informática no cuenta con salidas de emergencia. Por lo cual se debería reestructurar otras salidas debidamente señalizadas, para evitar cualquier tipo de daños a la integridad física del personal.

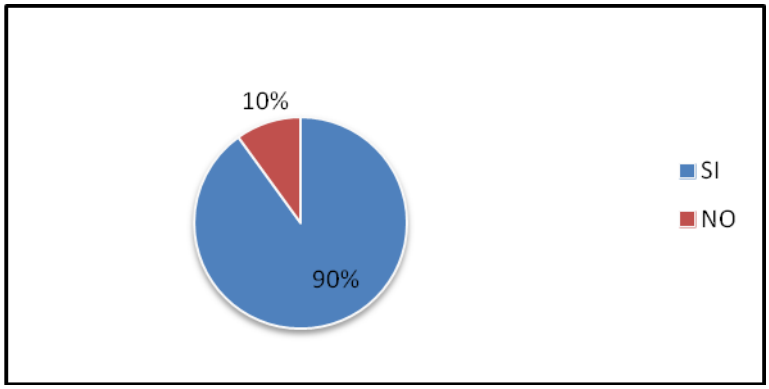
3.- ¿Los interruptores de energía eléctrica están debidamente protegidos, etiquetados, sin obstáculos para alcanzarlos?

TABLA 6. INTERRUPTORES DE ENERGÍA ELÉCTRICA

ALTERNATIVAS	FRECUENCIA	PORCENTAJES
SI	9	90%
NO	1	10%
TOTAL	**10**	**100%**

Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

GRÁFICO 6. INTERRUPTORES DE ENERGÍA ELÉCTRICA



Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

ANÁLISIS E INTERPRETACIÓN

De las 10 personas encuestadas en la División Redes 9 empleados que representa el 90% manifestaron que los interruptores de energía eléctrica están debidamente protegidos, etiquetados, sin obstáculos para alcanzarlos; mientras que 1 empleado que representa el 10% manifiesta lo contrario. En base a lo manifestado por la mayoría de los encuestados y lo observado por el grupo investigador se puede corroborar y afirmar el adecuado manejo de los interruptores de energía eléctrica.

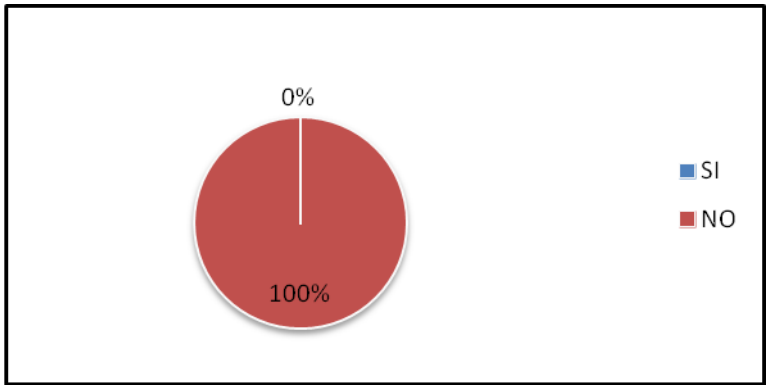
4.- ¿Se ha preparado a todo el personal en la forma en que se debe desalojar las instalaciones en caso de emergencia?

TABLA 7. PREPARACIÓN DEL PERSONAL

ALTERNATIVAS	FRECUENCIA	PORCENTAJES
SI	0	0%
NO	10	100%
TOTAL	**10**	**100%**

Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

GRÁFICO 7. PREPARACIÓN DEL PERSONAL



Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

ANÁLISIS E INTERPRETACIÓN

De los 10 empleados encuestados en la División Redes los 10 empleados que representan el 100% indican que no están preparados en la forma en que se debe desalojar las instalaciones en caso de emergencia. Por lo tanto los funcionarios de la institución deberían ofrecer una capacitación o simulacro para el desalojo del edificio ya que esto servirá de mucho para salvaguardar la integridad física del personal.

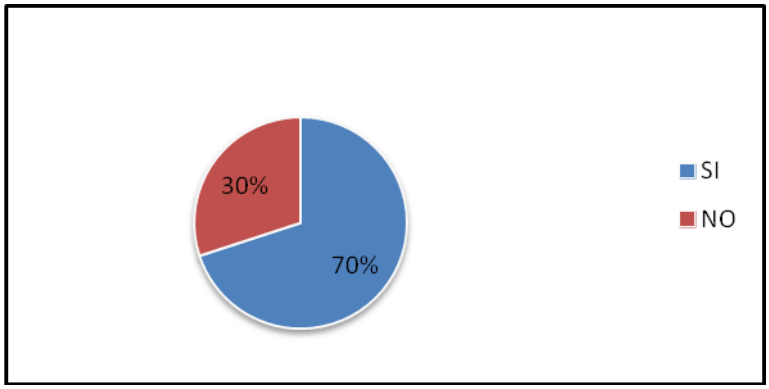
5.- ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?

TABLA 8. COPIAS DE LOS ARCHIVOS

ALTERNATIVAS	FRECUENCIA	PORCENTAJES
SI	7	70%
NO	3	30%
TOTAL	**10**	**100%**

Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

GRÁFICO 8. COPIAS DE LOS ARCHIVOS



Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

ANÁLISIS E INTERPRETACIÓN

De las 10 personas encuestadas en la División Redes 7 empleados que representan el 70% si cuenta con copias de los archivos en un lugar distinto al de la computadora; mientras que 3 empleados que representan al 30% no tiene documentos de respaldo.

Por lo tanto todos los encargados del manejo de la información deben tener respaldos en otras fuentes seguras y así evitar posibles pérdidas de información ante cualquier imprevisto.

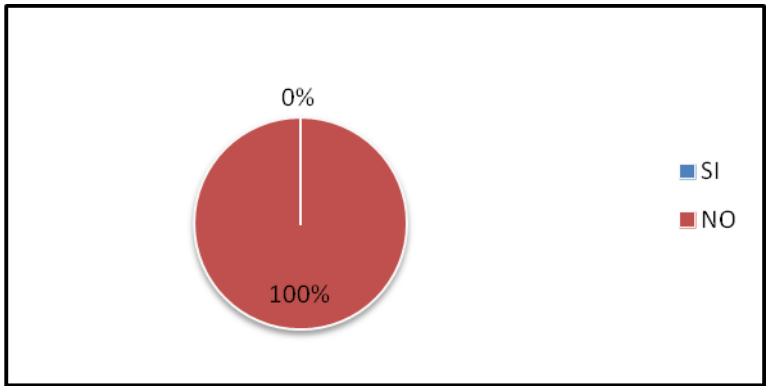
6.- ¿Tiene conocimiento de la existencia de un plan de contingencias?

TABLA 9. PLAN DE CONTINGENCIA

ALTERNATIVAS	FRECUENCIA	PORCENTAJES
SI	0	0%
NO	10	100%
TOTAL	**10**	**100%**

Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

GRÁFICO 9. PLAN DE CONTINGENCIA



Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

ANÁLISIS E INTERPRETACIÓN

De las 10 personas encuestadas en la División Redes los 10 empleados que representan al 100% mencionan que no tienen conocimiento de la existencia de un Plan de Contingencias. Por lo tanto se recomienda la elaboración inmediata de un Plan de Contingencia ya que es un instrumento de gestión para el buen desempeño de las Tecnologías de la Información y las Comunicaciones en el dominio del soporte; además contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad y operatividad de la institución.

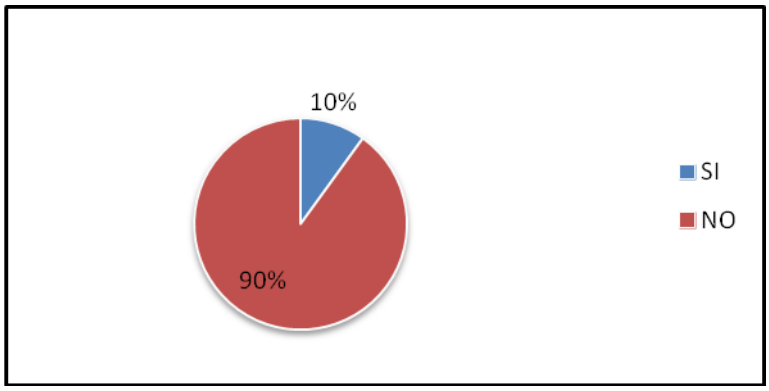
7.- ¿Los cables de red, switch, hubs, etc. se encuentran debidamente etiquetados?

TABLA 10. CABLES DE RED, SWITCH, HUBS

ALTERNATIVAS	FRECUENCIA	PORCENTAJES
SI	1	10%
NO	9	90%
TOTAL	**10**	**100%**

Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

GRÁFICO 10. CABLES DE RED, SWITCH, HUBS



Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

ANÁLISIS E INTERPRETACIÓN

De los 10 empleados encuestados en la División redes 1 empleado que representa al 10% manifiesta que los cables de red, switch, hubs, etc. se encuentran debidamente etiquetados; mientras que 9 empleados representan al 90% mencionan que los cables no se encuentran debidamente etiquetados. Por lo cual se recomienda la utilización de etiquetas que incluyan un identificador de sala y un identificador de conector, así se sabe todo sobre el cable: dónde empieza y dónde acaba.

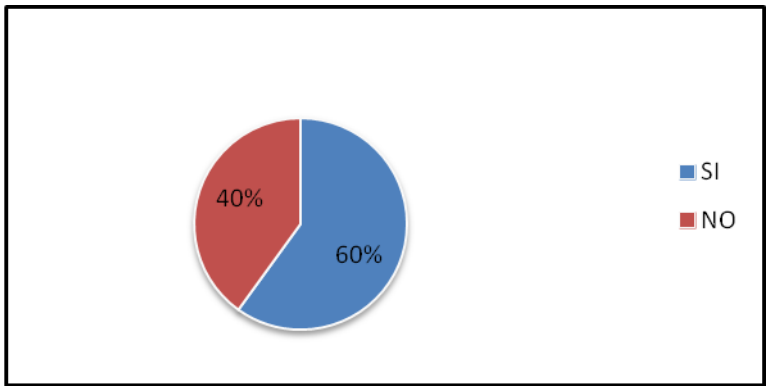
8.- ¿Se hace mantenimiento periódico a los computadores?

TABLA 11. MANTENIMIENTO DE COMPUTADORAS

ALTERNATIVAS	FRECUENCIA	PORCENTAJES
SI	6	60%
NO	4	40%
TOTAL	**10**	**100%**

Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

GRÁFICO 11. MANTENIMIENTO DE COMPUTADORAS



Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

ANÁLISIS E INTERPRETACIÓN

De los 10 empleados encuestados en la División Redes 6 empleados que representan el 60% manifiestan que si se hace mantenimiento periódico a los computadores; mientras que 4 empleados que representan al 40% revela que no ha existido mantenimiento a los equipos de cómputo. La División Redes cuenta con técnicos propios que se encargan del mantenimiento de los equipos de cómputo, una vez acabado el tiempo de las garantías de los equipos; dicho mantenimiento lo realizan en base a las necesidades que se presenten.

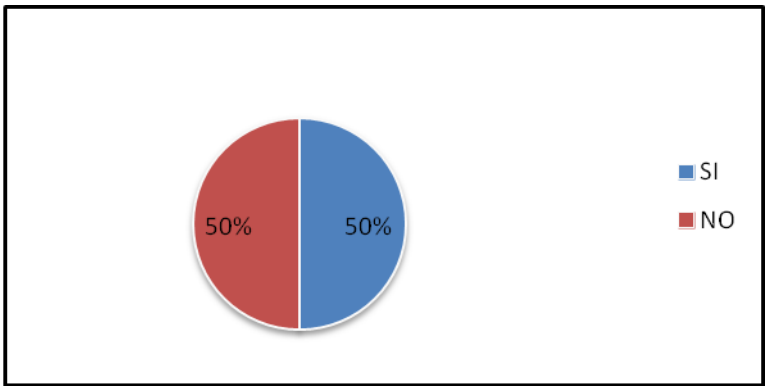
9.- ¿Se tiene reguladores para el equipo de cómputo?

TABLA 12. REGULADORES PARA EQUIPO DE CÓMPUTO

ALTERNATIVAS	FRECUENCIA	PORCENTAJES
SI	5	50%
NO	5	50%
TOTAL	**10**	**100%**

Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

GRÁFICO 12. REGULADORES PARA EQUIPO DE CÓMPUTO



Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

ANÁLISIS E INTERPRETACIÓN

De los 10 empleados encuestados en la División Redes 5 empleados que representan al 50% manifiestan que si tienen reguladores para el equipo de cómputo; mientras que 5 empleados que representan al 50% manifiestan que no tiene regulador para los equipos. Por lo tanto se ha observado que si cuentan con UPS que ayudan a regular y proporcionar energía por un tiempo limitado, permitiendo de esta manera guardar la información.

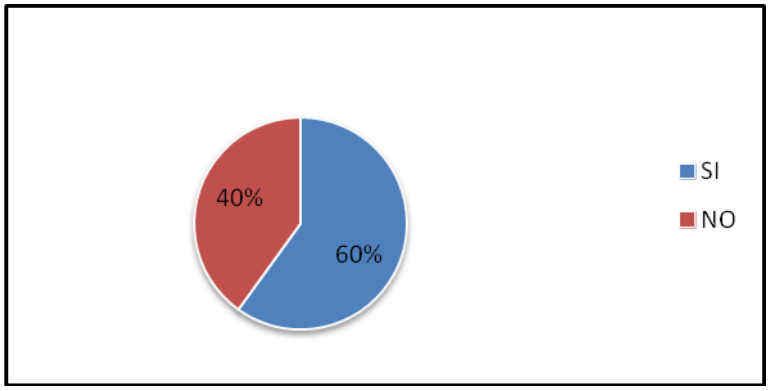
10.- ¿Se cuenta con tierra física**?**

TABLA 13. TIERRA FÍSICA

ALTERNATIVAS	FRECUENCIA	PORCENTAJES
SI	6	60%
NO	4	40%
TOTAL	**10**	**100%**

Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

GRÁFICO 13. TIERRA FÍSICA



Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

ANÁLISIS E INTERPRETACIÓN

De los 10 empleados encuestados en la División Redes 6 empleados que representan al 60% manifiestan que si cuentan con tierra física; y 4 empleados que representan el 40% lo desconocen. Se ha podido constatar en base a lo observado que la División Redes si cuenta con una conexión a tierra física, debido a que es un sistema de protección al usuario, de los aparatos conectados a la red eléctrica.

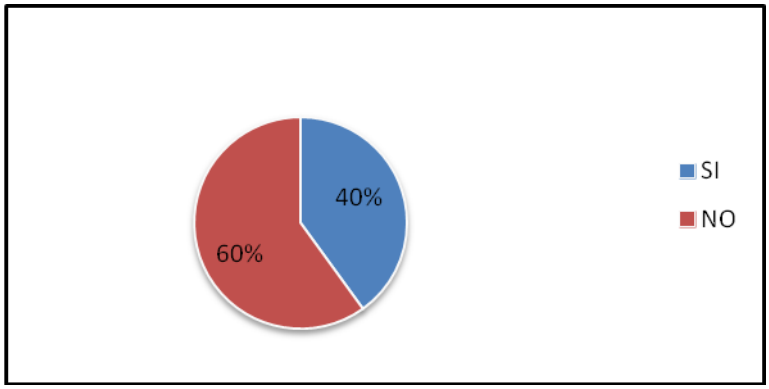
11.- ¿Existe un lugar suficiente para los equipos?

TABLA 14. LUGAR SUFICIENTE PARA LOS EQUIPOS

ALTERNATIVAS	FRECUENCIA	PORCENTAJES
SI	4	40%
NO	6	60%
TOTAL	**10**	**100%**

Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

GRÁFICO 14. LUGAR SUFICIENTE PARA LOS EQUIPOS



Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

ANÁLISIS E INTERPRETACIÓN

De los 10 empleados encuestados en la División Redes 4 empleados que representan el 40% mencionan que si existe un lugar suficiente para los equipos, mientras que 6 empleados que representan el 60% menciona que en la actualidad no cuentan con suficiente espacio para los equipos. En base a las encuestas aplicadas y a lo observado se pudo constatar que la División Redes no tiene suficiente espacio para sus equipos debido a que el lugar donde se encuentra es muy pequeño.

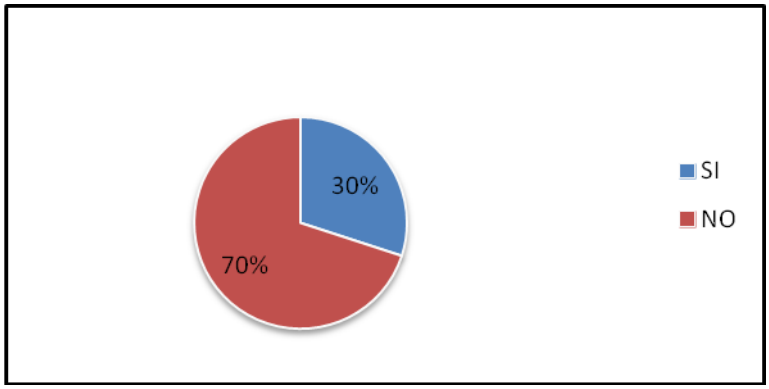
12.- ¿El piso es Antiestático?

TABLA 15. PISO ANTIESTÁTICO

ALTERNATIVAS	FRECUENCIA	PORCENTAJES
SI	3	30%
NO	7	70%
TOTAL	**10**	**100%**

Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

GRÁFICO 15. PISO ANTIESTÁTICO



Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

ANÁLISIS E INTERPRETACIÓN

De los 10 empleados encuestados en la División Redes 3 empleados que representan el 30% mencionan que si cuenta con un piso Antiestático; pero 7 empleados que representan el 70% mencionan lo contrario. Se observa que si tienen piso antiestático únicamente donde se encuentran los equipos que pertenecen al Sistema Troncalizado.

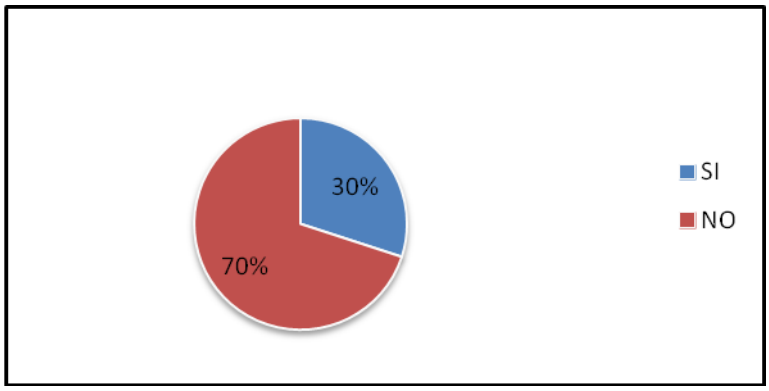
13.- ¿Los ductos del aire acondicionado están limpios?

TABLA 16. AIRE ACONDICIONADO

ALTERNATIVAS	FRECUENCIA	PORCENTAJES
SI	3	30%
NO	7	70%
TOTAL	**10**	**100%**

Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

GRÁFICO 16. AIRE ACONDICIONADO



Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

ANÁLISIS E INTERPRETACIÓN

De los 10 empleados encuestados en la División Redes 3 empleados que representan el 30% indican que los ductos del aire acondicionado están limpios, mientras que 7 empleados que representan el 70% manifiestan que los ductos del aire acondicionado están sucios. Se ha tomado en cuenta la opinión del Jefe de la División Redes que el aire acondicionado se encuentra en perfectas condiciones debido a que realizan mantenimiento una vez al año y el edificio donde se encuentra es nuevo por ende se encuentra limpio y en perfectas condiciones.

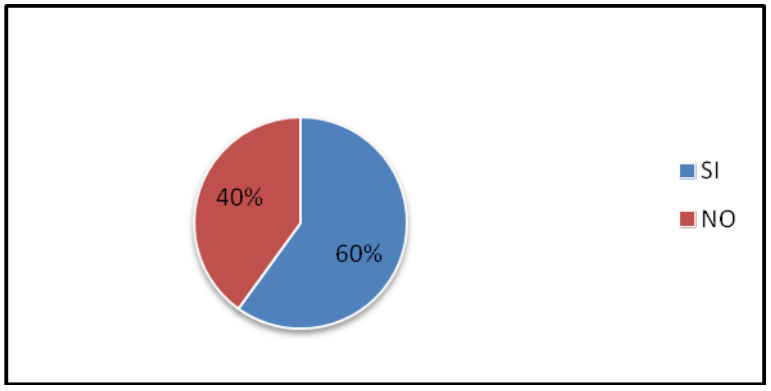
14.- ¿La temperatura en que trabajan los equipos es la recomendada por los proveedores?

TABLA 17. TEMPERATURA EN QUE TRABAJAN LOS EQUIPOS

ALTERNATIVAS	FRECUENCIA	PORCENTAJES
SI	6	60%
NO	4	40%
TOTAL	**10**	**100%**

Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

GRÁFICO 17. TEMPERATURA EN QUE TRABAJAN LOS EQUIPOS



Fuente: Personal de la D. N .T. I
Elaborado: Las tesistas

ANÁLISIS E INTERPRETACIÓN

De los 10 empleados encuestados en la División Redes 6 empleados que representan el 60% menciona que temperatura en que trabajan los equipos es la recomendada por los proveedores, mientras que 4 empleados que representan el 40% menciona que la temperatura en las que operan los equipos no es la adecuada. Por lo tanto la mayoría muestra conformidad con la temperatura en que operan los diferentes equipos cabe recalcar que se mantiene la temperatura que recomienda el proveedor ya que en caso de no realizarlo pierden la garantía entregada.

2.12. Conclusiones

Una vez finalizado el trabajo de resumen, análisis e interpretación de la información recopilada, fue posible llegar a las siguientes conclusiones:

- ✓ La División Redes de la Dirección Nacional de Telecomunicaciones e Informática carece de un sistema de Control Interno bien diseñado que tenga políticas, que les permita cuidar sus activos de forma física considerando que estos son la fuente de trabajo para su personal ocasionando malestar, daños y perjuicios, esto debido a que desde su creación no se ha realizado ningún tipo de Auditoría Informática.

- ✓ Al realizar la investigación dentro de la División Redes se pudo encontrar que no cuenta con un Plan de Contingencia, dicha institución no está preparada para cualquier tipo de desastres naturales o humanos.

- ✓ Dentro de la División Redes se pudo observar que, no cuenta con salidas de emergencias misma que puede ser causante de pérdidas humanas, en el caso de un accidente ya que ser humano es un factor importante dentro de una institución.

- ✓ Se verifica que en su mayoría, la infraestructura del edificio se encuentra deteriorada y no cumple con todas las medidas de seguridad que debería existir, ocasiona molestias al personal que labora dentro de la misma.

2.13. Recomendaciones

- ✓ Realizar una Auditoría a la Seguridad Física la cual ayudara a fortalecer la organización interna de la institución, garantizando eficiente y eficazmente el uso de los equipos e instalaciones.

- ✓ Elaborar un Plan de Contingencia, por lo menos anualmente el mismo que servirá para salvaguardar cada uno de los equipos, información, y al Talento Humano con que cuenta la institución.

- ✓ Señalar las diferentes salidas de emergencia que tiene la institución y ofrecer una capacitación adecuada al personal para la evacuación del edificio y de esta manera se protegerá la integridad física del personal.

- ✓ Observar en su totalidad la seguridad de la infraestructura física de la D.N.T.I. ya que no está acorde a las necesidades del personal que labora dentro de dicha institución.

CAPÍTULO III

"AUDITORÍA INFORMÁTICA A LA SEGURIDAD FÍSICA EN LA DIVISIÓN REDES DE LA DIRECCIÓN NACIONAL DE TELECOMUNICACIONES E INFORMÁTICA DE LA POLICÍA NACIONAL, DE LA CIUDAD DE QUITO, AL PERÍODO DEL 1 DE OCTUBRE DEL 2012 AL 31 DE ENERO DEL 2013"

3. Diseño de la Propuesta

3.1. Introducción

La Auditoría física evidencia que se tenga siempre una lista de los usuarios, es decir identifica que realmente se deje un avance o documentación sobre el acceso a la información y bases de datos en general.

El capítulo se enfoca en el desarrollo de una práctica de Auditoría Informática a la Seguridad Física en la División Redes de la Dirección Nacional de Telecomunicaciones e Informática de la Policía Nacional. Se aplica todos los conocimientos teóricos sobre el tema, además se pone en práctica la metodología con la que cuenta el desarrollo de una Auditoria Informática a la Seguridad Física.

Se presenta un esquema de los planes y programas para ejecutar las diferentes tareas para el análisis de cada una de las áreas críticas determinadas; cuyo objetivo principal es organizar todas las actividades evitando de este modo la duplicación de tareas, la información y evidencias, son recolectadas aplicando diferentes técnicas de auditoría;

de estos resultados depende la determinación de hallazgos, los cuales son la base para la obtención de conclusiones y recomendaciones.

Como resultado se genera una opinión técnica objetiva con respecto al nivel de seguridad de la información dentro del centro de datos, adicional a esto se detalla las debilidades encontradas y se emite las recomendaciones que contribuyan a mejorar los controles en cuanto a seguridad física del centro de datos.

3.2. Justificación

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

Siendo así la Dirección Nacional de Telecomunicaciones e Informática la encargada de brindar asesoramiento en el área tecnológica a la Policía Nacional y a su vez una Institución Pública, se debe tener en cuenta las Leyes que rigen el manejo de las Empresas Públicas, estas leyes se encuentran dictadas por la Contraloría General del Estado.

Además la ejecución de una Auditoría a la Seguridad Física, permitirá una evaluación objetiva de la seguridad de los recursos tecnológicos y así fortalecer sus conocimientos, brindando de esta manera un aporte a la investigación en temas relacionados con Auditoría Informática.

Con referencia a lo anterior, resulta conveniente realizar una Auditoría a la Seguridad Física al centro de datos de la División Redes, con la finalidad de evaluar el estado actual de los equipos informáticos, identificando los posibles riesgos, recomendando acciones de mejoras para el manejo y seguridad de los equipos tecnológicos y del personal que labora, salvaguardando de esta manera los equipos públicos y poder seguir con el desarrollo normal de las actividades.

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

Y conociendo que la División Redes es consciente que los procesos que se llevan a cabo son importantes para la institución y que la protección de los recursos tecnológicos es imprescindible, las autoras justifican el tema ya mencionado, mediante la metodología de la Auditoría a la Seguridad Física que se basan en normas nacionales e internacionales.

3.3. Objetivos

3.3.1. Objetivo General

Determinar las fases para el desarrollo de una Auditoría a la Seguridad Física con su aplicación en la División Redes de la Dirección Nacional de Telecomunicaciones e Informática del Cantón Quito, que permita emitir un informe con conclusiones y recomendaciones favoreciendo a la utilización de los equipos e instalaciones de la institución.

3.3.2. Objetivos Específicos

- ✓ Establecer la Metodología a utilizar para la correcta aplicación de la Auditoría a la Seguridad Física, realizándola en forma secuencial y ordenada.
- ✓ Determinar los hallazgos para la elaboración de la estructura del informe a presentar, efectuar el seguimiento del cumplimiento de recomendaciones.
- ✓ Establecer conclusiones y recomendaciones que permitan mejorar la seguridad de los equipos e instalaciones a través de la presentación de un informe.

3.4 Descripción de la Propuesta

En la División Redes, una de las funciones más importantes es administrar y mantener operativo los diferentes sistemas de comunicaciones, disponiendo del recurso humano y los medios técnicos necesarios en beneficio de la colectividad, lo cual permite crear y mantener un ambiente adecuado para la ciudadanía.

Se presenta un esquema de los planes para ejecutar las diferentes tareas para el análisis de cada una las áreas críticas determinadas; los programas son diseñados en base al modelo conceptual de la metodología presentada en el primer capítulo.

Las actividades se las ha organizado en tablas en donde consta el número de tareas, actividades, lugar en donde debe realizarse, objetivo que se pretende alcanzar con el cumplimiento de la tarea, técnicas e instrumentos a utilizarse para la recopilación y análisis de la información recolectada.

Después de cada plan cumplido se redactara un informe de las tareas desarrolladas, haciendo constar los motivos del incumplimiento de determinadas tareas si fuere el caso, toda la información recolectada es analizada para obtener una apreciación del estado del segmento auditado.

La información y evidencia son recolectados aplicando diferentes técnicas de auditoría; de los resultados de cada una de las tareas ejecutadas depende la determinación de los hallazgos, los cuales son la base para la obtención de conclusiones y recomendaciones.

Finalmente en la fase de comunicación de resultados se elaborará el borrador del informe a ser discutido con los directivos de la institución hasta llegar al definitivo, este informe se preparará una vez obtenidas y analizadas las respuestas de compromiso de cumplir con cada recomendación emitida.

La ordenación de las áreas, carpetas se realizaran de manera ordenada y lógica con el fin de permitir su fácil localización.

3.5 Desarrollo de la propuesta

3.5.1. Archivo Permanente

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
ÍNDICE DEL ARCHIVO PERMANENTE
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

F I

	CONTENIDO	REF.
	Programa de Auditoría	P/A 1/9
AP1	**INFORMACIÓN GENERAL**	
1.1	Reseña Histórica	R/H 1/5
1.2	Dirección de la matriz, y Horarios de trabajo.	D/H 1/1
1.3	Escritura de Constitución y Estatutos.	E/C 1/12
1.4	Personal directivo.	P/D 1/1
AP2	**ACTIVIDADES INSTITUCIONALES**	
2.1	Servicios que ofrece la Institución	S/O.I 1/1
AP3	**INFORMACIÓN DE INSTALACIONES, EQUIPOS Y PERSONAL**	
3.1	Principales departamentos o secciones, con una breve indicación de sus funciones y número de personas que los conforman.	D/F 1/1
3.2	Detalle de Equipos informáticos que posee la institución	E/I 1/1
AP4	**MANUALES DE PROCEDIMIENTOS Y FLUJOGRAMAS**	D/F 1/1
4.1	Organigrama estructural.	E/I 1/1
4.2	Proceso de Mantenimiento de Equipos de cómputo	F/M 1/1
4.3	Proceso de Programación de Equipos cómputo	F/P 1/1
4.4	Proceso de Instalación de Equipos tipo Base y Móviles	F/I 1/1

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 21-10-2012
REVISADO POR: L.F.P.G	FECHA: 21-10-2012

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
PROGRAMA DE AUDITORÍA
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

P/A 1/9

OBJETIVO

- ✓ Verificar los componentes a auditarse, mediante la aplicación de procedimientos, garantizando que las instalaciones y equipos tengan un lugar apropiado para su funcionamiento.

Nº	PROCEDIMIENTO	REF. P/T	ELABORADO POR:	
			AUDITOR	FECHA
1	Solicitar toda la documentación necesaria existente, organigrama estructural, funcional, base legal de creación, manuales, procedimientos, instructivos, reglamentos y más documentación que ringa las actividades informáticas relacionadas a la Seguridad Física.	R/H 1/5 D/H 1/1 E/C 1/18	Consulexter S.A	05-11-2012
2	Solicitar información sobre los principales departamentos o secciones, con una breve indicación de sus funciones y número de personas que los conforman	D/F 1/1	Consulexter S.A	07-11-2012
3	Solicitar un detalle de los Equipos informáticos que posee la institución.	E/I 1/5	Consulexter S.A	08-11-2012
4	Solicitar los flujogramas de los diferentes procesos que se realiza en la División Redes.	F/M 1/1 F/P 1/1 F/I 1/1	Consulexter S.A	12-11-2012

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 05-11-2012
REVISADO POR: L.F.P.G	FECHA: 05-11-2012

1.1. RESEÑA HISTÓRICA

La Ley Orgánica de la Policía Nacional en su Art. 53 del año 1998, crea la Dirección Nacional de Comunicaciones, y mediante RESOLUCIÓN No. 2000-353-CG-P.N. del 3 de Octubre del 2000 Aprueba y expedir el Reglamento Orgánico - Funcional de la Dirección Nacional de Comunicaciones de la Policía Nacional.

En el año 2000 la Dirección Nacional de Comunicaciones funcionaba en el Rancho San Vicente en las Oficinas pertenecientes al Club de Oficiales de la Policía Nacional junto a la Escuela de Especialización y Perfeccionamiento de Oficiales, bajo una estructura orgánica muy básica.

En el año 2001, posterior a la aprobación del Orgánico Funcional, la Dirección Nacional de Comunicaciones arrienda un edificio en las Calles José Ortón y Paúl Rivet para el funcionamiento técnico administrativo de conforme a la nueva estructura organizacional aprobada.

En el año 2002 el señor Crnl. Ing. Carlos Grijalva Director Nacional de Comunicaciones, realiza las gestiones respectivas ante el Ministerio de finanzas y consigue en calidad de Comodato por 50 años una Infraestructura física ubicada en el sector la Gasca, sitio estratégico desde el punto de vista técnico.

Se realiza las adecuaciones y mantenimiento de la infraestructura física de la edificación otorgada en Comodato

Desde el año 2003 hasta la presente fecha el Centro de Datos de la Dirección Nacional de Telecomunicaciones, funciona en las calles Rither Oe 9-141 y Diego Zorrila sector La Gasca.

BASE LEGAL:

La Dirección Nacional de Telecomunicaciones e Informática, fue creada del 3 de octubre del 2000. Rigen sus funciones y actividades las siguientes Leyes:

- ✓ La Ley Orgánica de la Policía Nacional
- ✓ Reglamento de Disciplina de la Policía
- ✓ Ley de Personal de la Policía Nacional
- ✓ Código de Ética Profesional de la Policía Nacional
- ✓ Código Penal de la Policía Nacional
- ✓ Reglamento de Régimen Interno de las Unidades Policiales
- ✓ Reglamento de Conformación y Funcionamiento de la Comisión de Adquisiciones de las Direcciones Generales y Nacionales, de los Comandos Provinciales y Unidades Especiales de la Policía Nacional.

MISIÓN

La Dirección Nacional de Comunicaciones tiene por misión liderar, la prestación de servicios de comunicaciones e informática dentro de la Policía Nacional, a través de una constante preparación del elemento humano y la utilización de la tecnología adecuada, que garantice la eficiencia y eficacia en su empleo, en el beneficio institucional y de la comunidad.

VISIÓN

Ser reconocida por el desarrollo e incorporación de tecnologías de información y comunicación mediante una capacitación permanente, investigación continua, una activa vinculación e innovación tecnológica con estándares de calidad que contribuyan a garantizar la seguridad y operatividad de los servicios informáticos y de comunicación.

OBJETIVOS ORGANIZACIONALES

OBJETIVO GENERAL

Desarrollar las funciones de comunicaciones e informática, para apoyar todas las labores de la Policía Nacional a fin de optimizar la gestión institucional

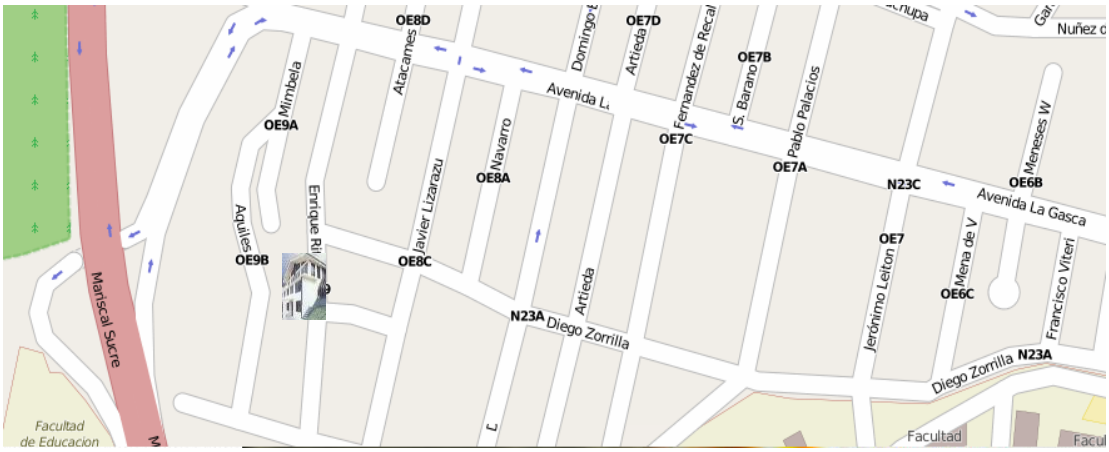
OBJETIVOS ESPECÍFICOS

- ✓ Lograr y mantener el más alto grado de calidad en los servicios de telecomunicaciones e informática de la Policía Nacional.
- ✓ Procurar la excelencia administrativa de la infraestructura existente en la Policía Nacional en materia de telecomunicaciones e informática.
- ✓ Estandarizar la infraestructura tecnológica.
- ✓ Centralizar las decisiones tecnológicas y descentralizar las acciones operacionales.
- ✓ Promover la modernización constante y del desarrollo continuo en los servicios de comunicaciones e informática.

1.2. DIRECCIÓN DE LA MATRIZ Y HORARIO DE TRABAJO

La Dirección Nacional de Telecomunicaciones e Informática "División Redes", se encuentra ubicada en la Provincia de Pichincha, Cantón Quito, calles Rither Oe 9-141 y Diego Zorrilla sector La Gasca,

Los horarios de trabajo son: de 8:00 am a 12:30 pm con una hora de almuerzo, y de 13:30 pm a 17:00 horas, además cuentan con una persona de turno rotativo que labora las 24 horas del día.



ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 05-11-2012
REVISADO POR: L.F.P.	FECHA: 05-11-2012

1.3. ESCRITURA DE CONSTITUCIÓN

ORDEN GENERAL Nº 191
DEL COMANDO GENERAL DE LA POLICÍA NACIONAL
PARA EL DÍA MARTES 3 DE OCTUBRE DEL 2000
RESOLUCIÓN DEL CONSEJO DE GENERALES

ART. 11º RESOLUCIÓN Nº. 00-353-CGPN.- EL CONSEJO DE GENERALES DE LA POLICÍA NACIONAL

Antecedentes.- El señor Comandante General de la Policía Nacional, mediante hoja de tramite Nº. 6520, de 9 de mayo del 2000, envía a este organismo para conocimiento y estudio, el proyecto del Reglamento Orgánico Funcional de la Dirección Nacional de Comunicaciones de la Policía Nacional.

CONSIDERANDO

Que, es atribución del Consejo de Generales de la Policía Nacional, aprobar la reglamentación interna de la Institución, conforme a lo dispuesto en el Artº. 22 literal d) de la Ley Orgánica de la Policial Nacional.
Que, en el Art. 53 literal k) de la Ley Orgánica de la Policial Nacional, se establece entre las Direcciones Nacionales de la Policía Nacional, la Dirección Nacional de Comunicación;
Que, es necesario modernizar la Administración policial, para alcanzar mejores índices de eficiencia operacional, especialmente en el área de comunicaciones e informática;
Que es necesario determinar la estructura, funciones y responsabilidades, que debe cumplir la Dirección Nacional de Comunicación de la Policía Nacional.

Que es función del Comando General, sancionar la reglamentación interna de la institución, previa resolución del Consejo de Generales de la Policía Nacional, conforme a lo establecido en el Art. 18, literal t) de la Ley Orgánica de la Policía Nacional.
Que el señor Director Nacional de Asesoría Jurídica de la Policía Nacional, mediante oficio Nº 20-2657-DNAJ-PN, DE 10 de agosto del 2000, emite su informe; y,
En uso de sus atribuciones legales y reglamentarias;

RESUELVEN:

1.- Aprobar el siguiente Reglamento Orgánico funcional de la Dirección Nacional de Comunicaciones de la Policía Nacional, de conformidad a lo dispuesto en el Art. 22 Literal d) de la Ley Orgánica de la Policía Nacional; y, solicitar al señor comandante General de la Policía Nacional, sancione el Reglamento antes indicado, de acuerdo a lo establecido en el artículo 18 literal t) del mismo cuerpo legal.

REGLAMENTO ORGÁNICO DE LA DIRECCIÓN NACIONAL DE COMUNICACIONES DE LA POLICÍA NACIONAL.

TITULO I
DE LA MISIÓN Y OBJETIVOS

ART1.- La Dirección Nacional de Comunicación, tiene por misión esencial liderar la prestación del servicio de comunicaciones e informática, a través de una constante preparación del elemento humano y la utilización de la tecnología adecuada que garantice la eficiencia y eficacia en su empleo en beneficio institucional y de la comunidad.
Art. 2.- Al a Dirección Nacional de Comunicación, le corresponde las funciones de comunicación e informática, para apoyo todas las labores de la Policial Nacional a fin de optimizar la gestión institucional.

Sus objetivos específicos son:

a) Lograr y mantener el más alto grado de calidad en los servicios de comunicaciones informáticas de la Policía Nacional;
b) Procurar la excelencia administrativa de la infraestructura existente de la Policía Nacional, en materia de comunicaciones e informática;
c) Estandarizar la infraestructura tecnológica;
d) Centralizar las decisiones tecnológicas y descentralizar las acciones operacionales en esta área;
e) Promover la modernización constante y el desarrollo continuo en los servicios de comunicación r informática; y,
f) Fortalecer la participación policial con la comunidad a través del asesoramiento en materia de comunicaciones e informática.

TITULO II
DE LA ESTRUCTURA ORGÁNICA

Art. 3.- La Estructura Orgánica de la Dirección Nacional, estará integrado por los siguientes niveles:
1. Nivel Directivo
2. Nivel Asesor
3. Nivel Administrativo
4.- Nivel técnico –Operativo

CAPITULO I
NIVEL DIRECTIVO

Art. 4.- El Nivel Directivo, es la máxima autoridad, le corresponde la toma de decisiones que la Dirección Nacional es requiera para el cumplimiento de sus funciones en el campo administrativo y operativo estará integrado por:
1. Dirección Nacional de comunicaciones
2.- Comité de Gestión de Calidad

CAPITULO II
NIVEL ASESOR

Art 5.- El Nivel Asesor, es el órgano consultivo para la toma de decisiones de la Dirección Nacional; estará integrado por:
1. Asesoría Técnica
2. Asesoría Jurídica

CAPITULO III
NIVEL ADMINISTRATIVO

Art 6.- El Nivel Administrativo, tiene a su cargo la gestión administrativa, lógica y financiera, proporciona los recursos necesarios para el cumplimiento de las funciones asignadas a la Dirección Nacional: estará integrado por.
1. Secretaria General
2. Departamento Administrativo, con las Secciones:
2.1. Personal
2.2 Logística
3. Departamento Financiero, con las Secciones:
3.1. Presupuesto
3.2 Contabilidad
3.3 Administración de Caja
3.4 Activos Fijos

CAPITULO IV
NIVEL TÉCNICO-OPERATIVO

Art 7.- El Nivel Técnico Operativo, es el encargado de ejecutar las decisiones y requerimientos del Nivel Directivo en cumplimiento de los objetivos de la Policial Nacional comunicaciones e informática; estará integrado por:

1. División Redes
1.1. Departamento de Operaciones
1.1.1. Sección Centro de proceso de Datos
1.1.2. Sección Implantación
1.1.3. Sección Asistencia al Usuario
1.1.4. Sección Servicios Especiales
1.2 Departamento de Ingeniería
1.2.1. Sección Desarrollo
1.2.2. Sección Mantenimiento Evolutivo
2. Coordinación
2.1 Primer Distrito
2.2. Segundo Distrito
2.3. Tercer Distrito
2.4. Cuarto Distrito

TITULO III
DE LA ESTRUCTURA FUNCIONAL
CAPITULO I
DE NIVEL DIRECTIVO
DE LA DIRECCIÓN NACIONAL DE COMUNICACIÓN

Art 8.- La Dirección Nacional de Comunicaciones, estará dirigida por un Oficial de Línea con el grado de Coronel en servicio activo, con título académico y especialización en Ingeniería Electrónica o Sistemas, designado por el Comandante General; quien cumplirá las siguientes funciones:

a) Adaptar decisiones y disponer su ejecución tendiente a cumplir los objetivos de carácter Institucional, resueltos por el mando Policial, en materia de comunicaciones e informática.

b) Tomar las resoluciones administrativas, para el cumplimiento de los correspondientes niveles que fueren necesarias para la ejecución de los fines propios de la Dirección Nacional:

c) Administra la Tecnología de comunicaciones e informática a nivel nacional, basada en una planeación estratégica dinámica, procesos de calidad total y mejoramiento continuo:

d) Asesorar al Mando institucional en el área de comunicaciones e informática:

e) Velar por la buena imagen de los servicios de comunicación e informática, ponderando los valores de carácter personal y técnico-profesional:
f) Suscribir convenios de cooperación técnica, financiera, de capacitación y otras áreas de Internet para la Dirección Nacional de Comunicaciones, con instituciones públicas y privadas nacionales y de países amigos, previa delegación expresa del Comandante General:
g) Propone a la Dirección General de Personal, los cambios, incorporaciones y contratación de personal especializado:
h) Elaborar y Supervisar el proceso de capacitación continua del personal:
i) Analizar y Aprobar el presupuesto anual de la Dirección Nacional y presentar al Superior a fin de que se incluya en el Presupuesto General de la Policía Nacional:
J) Gestionar la adquisición de los recursos financieros extra presupuestarios que permite incrementar los fines propuestos.
k) Supervisar las actividades técnicas y administrativas de la Dirección Nacional:
l) Aprobar las Normas internas, tendientes a mejorar los procesos de los servicios comunicaciones e informática a través del desarrollo humano y organizacional:
m) Coordinar las tareas que ejecuta la Dirección Nacional, con las demás dependencias de carácter institucional e Interinstitucional, que permitan una gestión óptica:
n) Elaborar Informes periódicos de las tareas cumplidas por la Dirección Nacional y enviar conocimiento del Escalón Superior; y,
o) Cumplir y hacer cumplir las Leyes y Reglamentos de la Institución y más normas legales vigentes y aquellas dispuestas por el Escalón Superior.

EL COMITÉ DE GESTIÓN DE CALIDAD

Art. 9. El Comité de Gestión de Calidad, estará integrado por el Directos Nacional quien lo presidirá y los directores de División; para su gestión permanente contara con un asesor experto en gestión de calidad cumplirá las siguientes funciones:
a) comprometer el esfuerzo interno y establecer el apoyo externo necesario, a fin de implantar el Sistema de Control de Calidad;

b) Ejecutar las acciones pertinentes para consolidar un sistema de administración de calidad, con base en las normas del ISO;
C) Difundir los objetivos del control de calidad, sus beneficios en la institución y sus costos;
d) Comprometer los esfuerzos de todo el personal Directivo, Técnico y Administrativo al cumplimiento de la misión a través de la implantación y desarrollo del sistema de administración de calidad;
e) Generar Actividades orientadas al mejoramiento continuo, incorporando estrategias genéricas y manteniendo un constante desarrollo del sistema de administración de calidad; y,
f) Propender a la obtención de la Certificación ISO correspondiente.

CAPITULO II
DEL NIVEL ASESOR

Art. 10 La Asesoría Técnica, estará dirigida por un profesional en Ingeniería Electrónica o Sistemas; con amplia experiencia en el área; cumpliendo las siguientes funciones:
a) Formular y actualizar el plan estratégico a tres años y programa anual de trabajo y someter a conocimiento y aprobación del señor Director.
b) Elaborar diagnósticos técnicos de las necesidades básicas en materia de comunicaciones e informática que requiere la Institución a nivel nacional.
c) Diseñar programas y proyectos técnicos de comunicación e informática, requeridos por la Institución Policial.
d) Realizar estudios técnicos, tendiente a establecer sitios estratégicos para enlaces de comunicaciones, de voz y datos:
e) Supervisar y evaluar los proyectos, dispuestos por la Dirección Nacional, de acuerdo a la prioridad técnica establecida;
f) Elaborar los proyectos informáticos, definir las fases y estándares para los requerimientos institucionales de aplicaciones de sistemas de información;
g) E laborar el componente técnico de los documentos precontractuales y de los contratos estándar, para provisión de bienes y servicios de comunicación e informática;

h) Analizar el mercado de comunicaciones e informática y conocer los principales fabricantes, productos, proveedores de bienes y servicios;
i) Delinear las políticas de desarrollo impartidas al equipo del proyecto;
j) Estandarizar parámetros en la codificación de programas;
k) Evaluar periódicamente los Proyectos ejecutados a nivel nacional y elaborar los informes correspondientes al Escalón Superior;
l) Proponer alternativas de mejoramiento técnico de las comunicaciones e informática en la Institución;
m) Proponer las recomendaciones técnicas, conforme a las evaluaciones respectivas;
n) Manejar el archivo técnico documental y biblioteca de la Dirección Nacional;
o) Planificar, dirigir, supervisar y evaluar los cursos de capacitación sobre las nuevas innovaciones tecnológicas, para el personal de la Dirección Nacional y del universo Institucional;
p) Programar el pensum de materias, duración y carga horaria de los cursos, de acuerdo el grado cultural y especialización del personal;
q) Definir las necesidades de capacitación y seleccionar al personal docente o empresas para los cursos de capacitación, considerando su profesión, experiencia docente, especialización, cursos de actualización y conocimiento pedagógico;
r) Mantener relaciones con Instituciones Superiores de Enseñanza y Centros de Capacitación del país y del exterior, a fin de mejorar la calidad de los cursos y la excelencia en la enseñanza-aprendizaje;
s) Coordinar con cada nivel de la estructura orgánica, para la programación de los cursos de capacitación;
t) Elaborar el presupuesto, para los diferentes cursos de capacitación, a dictarse en un año;
u) Elaborar informes sobre las evaluaciones de los cursos de capacitación, para conocimiento y decisión del Director;
v) Elaborar informes periódicos de las tareas cumplidas y enviar a conocimiento del Escalón Superior, y;
w) Cumplir con las demás funciones previstas en la Ley y aquellas dispuestas por el Escalón.

Art. 11.- La Asesoría Jurídica, estará a cargo de un Oficial del Servicio de Justicia de la Policía Nacional, designado por el Comandante General; cumplirá las siguientes funciones:
a) Asesorar a la Dirección Nacional, en el área jurídica;
b) Estudiar y emitir informes de carácter legal, sobre los asuntos que sean sometidos a su conocimiento;
c) Elaborar y revisar con criterio jurídico los proyectos de convenios, documentos precontractuales o contratos, de conformidad con la Ley, y supervisar el cabal cumplimiento y ejecución;
d) Recopilar y mantener actualizada la legislación pertinente a las actividades que ejecuta la Dirección Nacional;
e) Elaborar informes periódicos de las tareas cumplidas y enviadas a conocimiento del Escalón Superior, y;
f) Cumplir con los demás funciones previstas en la Ley y aquellas dispuestas por el Escalón Superior.

CAPITULO III
DEL NIVEL ADMINISTRATIVO
SECCIÓN I

Art. 12.- La Secretaria General, se subordina directamente al Director Nacional, estará a cargo de un Clase, Titulado, con experiencia en esta área; cumplirá las siguientes funciones:
a) Recibir, registrar y despachar la correspondencia de la Dirección Nacional;
b) Elaborar oficios, informes, memorandos, telegramas y demás documentos requeridos por el Escalón Superior y enviar a los destinatarios;
c) Mantener actualizado el registro de las autoridades y funciones del Gobierno Nacional y de la Institución; al igual que, la guía telefónica y direcciones electrónicas de las Unidades Policiales a nivel Nacional e información de los miembros de la Institución;
d) Registrar y controlar la documentación procesada en la Dirección Nacional, a fin de informar sobre el trámite dado;
e) Mantener el archivo de la Dirección Nacional, conforme a las normas técnicas y de confidencialidad exigidas;

f) Eliminar, previa autorización del Escalón Superior y de conformidad, con las disposiciones legales vigentes, los documentos que haya perdido su valor utilitario para la Dirección Nacional;
g) Elaborar informes periódicos de las tareas cumplidas y enviadas a conocimiento del Escalón Superior; y,
h) Cumplir con las demás funciones previstas en la Ley y aquellas dispuestas por el Escalón Superior.

PARAGRAFO 1

Art. 13.- El Departamento Administrativo, estará dirigido por un Oficial de Policía de Línea, con experiencia en tareas administrativas y logísticas, cumplirá las siguientes funciones:
a) Administrar los procesos relacionados al personal la logística y la documentación de la Dirección Nacional;
b) Supervisar la recepción, clasificar, registros y archivos de los documentos que ingresen a la Dirección Nacional;
c) Tramitar y despachar los documentos y comunicaciones, dispuestos por el Director Nacional;
d) Conferir copias certificadas de documentos solicitados, previa autorización del Directos Nacional;
e) Dirigir y supervisar las acciones en materia de Personal y Logística, de un modo integral;
f) Elaborar informes periódicos de las tareas cumplidas y enviar a conocimiento del Escalón Superior; y,
g) Cumplir con las demás funciones previstas y aquellas dispuestas por el Escalón Superior.

PARAGRAFO 2

Art. 12.- La Sección Personal, estará a cargo de una clase con experiencia en esta área; cumplirá las siguientes funciones:
a) Dirigir, supervisar y controlar el elemento humano, conforme a la Ley de Personal, su Reglamento y disposiciones del Escalón Superior, e, informar de su situación;
b) Dirigir y supervisar el proceso de selección de personal, registro, clasificación, valoración y evaluación del elemento humano de la Dirección Nacional;
c) Asesorar al Escalón Superior en materia de administración del talento humano;

d) Conferir copias certificadas de documentos solicitados, previa autorización del Directos Nacional;
e) Dirigir y supervisar las acciones en materia de Personal y Logística, de un modo integral;
f) Elaborar informes periódicos de las tareas cumplidas y enviar a conocimiento del Escalón Superior; y,
g) Cumplir con las demás funciones previstas y aquellas dispuestas por el Escalón Superior.

PARAGRAFO 2

Art. 12.- La Sección Personal, estará a cargo de una clase con experiencia en esta área; cumplirá las siguientes funciones:
a) Dirigir, supervisar y controlar el elemento humano, conforme a la Ley de Personal, su Reglamento y disposiciones del Escalón Superior, e, informar de su situación;
b) Dirigir y supervisar el proceso de selección de personal, registro, clasificación, valoración y evaluación del elemento humano de la Dirección Nacional;
c) Asesorar al Escalón Superior en materia de administración del talento humano;
d) Mantener actualizada; la información referente a personal: nomina, licencias, permisos, comisiones, vacantes y requerimientos;
e) Hacer conocer al personal de las disposiciones emanadas por el Director Nacional, destacando el cumplimiento a cabalidad mediante el trabajo en equipo;
f) Actualizar las normas internas de administración de personal, e informar al Escalón Superior;
g) Aplicar las políticas impartidas por el Director Nacional, mediante acciones encaminadas a elevar el nivel de desempeño del personal;
h) Coordinar acciones con los Departamentos de la Dirección Nacional, a fin de evaluar de un modo permanente, la actividad y actitud del talento humano, para promover un trabajo conjunto de mejoramiento continuo;
i) Elaborar informes periódicos de las tareas cumplidas y enviar a conocimiento del Escalón Superior; y,
j) Cumplir con las demás funciones previstas en la Ley y aquellas por el Escalón Superior.

PARAGRAFO 3

ART. 15.- La Sección Logística, estará a cargo de un Clase con experiencia en esta área: cumplirá las siguientes funciones:

a) Establecer y controlar las necesidades logísticas a nivel nacional;

b) Administrar la obtención, almacenamiento, transporte y posterior distribución del material, a las Unidades pertenecientes a la Dirección Nacional;

c) Gestionar la adquisición, construcción y mantenimiento de las instituciones policiales, de la Dirección Nacional;

d) Planificar la obtención y facilitación de servicios;

e) Registrar y controlar los diferentes tipos de abastecimiento, nivel de existencia, fecha de caducidad, necesidad de mantenimiento y cambios de ubicación;

f) Supervisar que las dependencias policiales pertenecientes a la Dirección Nacional, mantenga sus abastecimientos en el nivel operacional y preverá el nivel de seguridad de acuerdo a las circunstancias;

g) Registrar y controlar el parque automotor;

h) Registrar y controlar el mantenimiento oportuno del parque automotor y armamento, ingreso y empleo de partes y piezas;

i) Planificar las reposiciones de abastecimiento y repuestos;

j) Elaborar informes periódicos de las tareas cumplidas y enviar a conocimiento del Escalón Superior; y,

k) Cumplir con las demás funciones previstas en la Ley y aquellas dispuestas por el Escalón Superior.

SECCION II

Art. 16.- El Departamento Financiero, estará dirigido `por un Oficial de Policía del Servicio de intendencia, con experiencia en tareas financieras contables; cumplirá las siguientes funciones:

a) Programar, organizar, dirigir, ejecutar, coordinar y controlar las actividades financieras contables de la Dirección Nacional, de conformidad con las Normas Legales vigentes, Reglamentos, Directivas e Instructivos, emitidos por el Escalón Superior;

b) Velar por el funcionamiento correcto del control interno, dentro de los sistemas de presupuesto, contabilidad de los recursos entregados a la Dirección Nacional;

c) Elaborar el presupuesto anual de la Dirección Nacional, en coordinación con la Dirección Nacional Financiera, observando las normas técnicas vigentes para el trámite al Escalón Superior;
d) Analizar los estados financieros, reportes de caja y otros informes, hacen observaciones y aplican los correctivos que fueren necesarios; debiendo informar del particular al Director Nacional;
e) Participar en avalúos, bajas, remates, entrega- recepción de los bienes de la Dirección Nacional;
f) Elaborar informes periódicos de las tareas cumplidas y enviadas a conocimiento del Escalón Superior; y,
g) Cumplir con las demás funciones previstas en la Ley y aquellas dispuestas por el Escalón Superior.

PARAGRAFO 1

Art. 17.- La Sección Presupuesto, estará a cargo de una clase con experiencia en esta área; cumplirá las siguientes funciones:
a) Determinar los recursos, necesarios reales, gastos corrientes, de capital, de inversión, y, a base de esta información, elaborar el proyecto anual de presupuesto de la Dirección Nacional y someter al estudio y aprobación del nivel superior;
b) Aplicar normas técnicas y administrativas.- presupuestarias, señaladas en la Ley, en los instructivos y manuales formulados por las Instituciones especializadas, así como las disposiciones dadas por el Jefe del Departamento Financiero;
c) Elaborar conjuntamente con la Unidad pertinente el proyecto de distributivos de sueldo del personal civil.
d) Presentar quincenalmente al Jefe del Departamento Financiero, el estado de ingresos y egresos, a fin de proceder al análisis correspondiente e introducir los correctivos pertinentes;
e) Aplicar sistemas específicos de evaluación financiera y presentar al Jefe del Departamento Financiero, informes trimestrales de los resultados obtenidos;
f) Elaborar mensualmente el balance de la Dirección Nacional y someter al trámite que la Ley determina;
g) Utilizar, los informes diseñados para el control de las partidas, así como aquellos que son fuente de información de las Operaciones de la Dirección Nacional;

h) Coordinar las tereas de la Unidad con las actividades que ejecutan las de Contabilidad, Administración de caja Y Activos Fijos;
i) Elaborar informes periódicos de las tareas cumplidas y enviar a conocimiento del Escalón Superior, y;
j) Cumplir con las demás funciones previstas en la Ley y aquellas dispuestas por el Escalón Superior.

PARAGRAFO 2

Art. 18.- La Sección de Contabilidad, estará a cargo de un Clase con experiencia en esta área; cumplirá las siguientes funciones:
a) Diseñar, organizar, aplicar y mantener el sistema de contabilidad, de conformidad con las normas legales vigentes, las expedidas por la Contraloría General del Estado, los principales de contabilidad generalmente aceptadas, la LOAFYC y las Directivas de la Dirección Nacional Financiera;
b) Mantener el control contable sobre los inventarios y activos fijos de la Dirección Nacional;
c) Preparar la documentación para la elaboración del rol de pagos del personal civil de la Dirección Nacional;
d) Elaborar comprobantes de pago, planillas de aporte y descuentos al IESS, retenciones judiciales y otros documentos que la Ley establece del personal civil de la Dirección Nacional;
e) Elaborar informes periódicos de las tareas cumplidas y enviadas a conocimiento del Escalón Superior; y,
f) Cumplir con las demás funciones previstas en la Ley y aquellas dispuestas por el Escalón Superior.

PARAGRAFO 3

Art. 19.- La Sección Administración de Caja, estará a cargo de un Clase con experiencia en esta área: cumplirá las siguientes funciones:
a) Administrar la unidad de caja en concordancia con las disposiciones legales vigentes y las normas expedidas por la Contraloría General del Estado y las disposiciones del Jefe del Departamento Financiero;
b) Registrar la firma conjuntamente con el Jefe del Departamento Financiero en los bancos oficiales o aquellos que la Ley permita, a fin cancelar las obligaciones contraídas por la Dirección Nacional;

c) Entregar los cheques a los beneficiarios, previa verificación y análisis de la legalidad de los documentos de respaldo;
d) Enviar a contabilidad en forma regular y sistemática, los comprobantes de depósito, en el orden cronológico en que fueron realizados, así como los documentos de las operaciones de la Dependencia;
e) Prepara el flujo de caja de la Dirección Nacional y presentar al Jefe del Departamento Financiero para su conocimiento y aprobación;
f) Llevar los libros de caja y bancos y los auxiliares necesarios, de conformidad con las normas legales vigentes y las directivas enviadas por la Dirección Nacional Financiera;
g) Elaborar informes periódicos de las tareas cumplidas y enviadas a conocimiento del Escalón Superior; y,
h) Cumplir con las demás funciones previstas en la Ley y aquellas dispuestas por el Escalón Superior.

PARAGRAFO 4

Art. 20.- L sección de activos Fijos, está a cargo de un Clase con experiencia en esta área; cumplirá las siguientes funciones;
a) Organizar y administra el sistema de control de los activos fijos de la Dirección Nacional, en concordancia con el Manual General DEL Estado y las Directivas para la Administración Y Control de los Activos Fijos, formulados por la Dirección Nacional Financiera;
b) Aplicar permanentemente el sistema de identificación, codificación, valoración y custodia de los bienes y activos fijos, emitidos por el Departamento de Control de Activos Fijos;
c) Intervenir en la suscripción de las respectivas actas, de la Dirección Nacional; exclusivamente en cuanto o donaciones, bajas, traspasos, por custodia temporal del bien u otras acciones observando las disposiciones de las leyes y normas vigentes;
d) Ejecutar periódicamente la toma física de inventarios por lo menos una vez al año;
e) Preparar informes previos, elaboración de detalles y actas de Inspección, antes de proceder al remate o baja de los artículos;
f) Elaborar informes periódicos de las tareas cumplidas y enviadas a conocimiento del Escalón Superior; y.

g) Cumplir con las demás funciones previstas en la Ley y aquellas dispuestas por el Escalón Superior.

CAPITULO IV
DEL NIVEL TÉCNICO-OPERATIVO
SECCIÓN I

Art. 21.- La División Redes, está dirigida por un Oficial, con título académico y especialización en Ingeniería Electrónica y Telecomunicaciones; cumplirá con las siguientes funciones;

a) Formular el programa anual de trabajo concordante al plan estratégico elaborado por la Asesoría Técnica y someter a conocimiento y aprobación del Escalón Superior.

b) Planificar, organizar, supervisar y evaluar los recursos técnicos, de todas las áreas informáticas de la Institución;

c) Supervisar permanentemente la ejecución de las tareas técnicas de mantenimiento;

d) Elaborar procesos de análisis administrativos, permanentes y recomendar su aplicación en las dependencias policiales;

e) Revisar los procedimientos de las dependencias a ser automatizadas y proponer su reorganización, de ser el caso:

f) Evaluar el rendimiento de las dependencias con fines técnicos e informáticos y proponer alternativas de organización;

g) Utilizar los medios técnicos de que dispone, para aportar a él o a los proyectos que la Dirección Nacional emprenda;

h) Propender a una estandarización de los recursos informáticos;

i) Mantener actualizados los inventarios de los recursos informáticos;

j) Realizar auditorías informáticas en las dependencias policiales que disponen del sistema y emitir el correspondiente informe técnico;

k) Realizar el análisis, diseño, desarrollo, implantación y mantenimiento evolutivo de los sistemas de información;

l) Administra los Centros de Proceso de Datos y la información de los Servicios Policiales, a través de grupos de trabajo dedicados;

m) Proponer el diseño, montaje y operacionalización del Hardware requeridos por la Institución;

n) Propiciar convenios de gestión participativa entra e interinstitucionales para efectos de soporte técnico y demás servicios asociados;

o) Dirigir las actividades técnicas de seguridad de la información, asignadas a la División;
p) Supervisar permanentemente el cumplimiento de los procedimientos y disposiciones aplicadas a la División;
q) Proponer controles administrativos y normas de seguridad personal;
r) Disponer la movilización de los técnicos de campo para realizar el trabajo requerido;
s) Supervisar permanentemente la ejecución de las tareas cumplidas y proponer alternativas para elevar sustancialmente los niveles de seguridad de los sistemas informáticos;
t) Coordinar con los demás componentes de la Dirección Nacional, a fin de mantener una filosofía concordante de trabajo en equipo;
u) Elaborar informes periódicos de las tareas cumplidas y enviar a conocimiento del Escalón Superior; y,
v) Cumplir con la demás funciones previstas en la Ley y aquellas dispuestas por el Escalón Superior.

SECCIÓN III

ART. 23.- La Coordinación de Distrito, estará dirigida por un Oficial, con título académico y especialización en Ingeniería Electrónica o de Sistemas; cumplirá las siguientes funciones:
a) Cumplir con las disposiciones emanadas por la Dirección Nacional y las Divisiones;
b) Facilitar las actividades de las Divisiones y Departamentos de la Policía Nacional;
c) Informar al área correspondiente de los avances en las tareas administrativas y técnico operacionales, en su jurisdicción;
d) Requerir el apoyo administrativo-logístico para el cumplimiento de sus actividades;
e) Formular acciones y proponer alternativas que conduzcan al logro de los objetivos de la Dirección Nacional;
f) Apoyar el cabal cumplimiento del sistema de Gestión de Calidad, en su jurisdicción;
g) Propiciar convenios de Gestión participativa intra e interinstitucionales para efectos de soporte técnico y demás servicios asociados;

h) Coordinar permanentemente con los Servicios y Dependencias policiales en su jurisdicción;
i) Coordinar con los demás componentes de la Dirección Nacional, a fin de mantener una filosofía concordante de trabajo el equipo;
j) Elaborar informes periódicos de las tareas cumplidas y enviadas a conocimiento del Escalón Superior; y,
Art. 24.- La Dirección Nacional de Comunicaciones, en lo referente a los Servicios Generales, se sujetara al Reglamento de Régimen Interno de la Unidades Policiales, aprobado y vigente por el mando policial.
Art. 25.- En relaciones a las adquisiciones, la Dirección Nacional se sujetará al Reglamento de Conforme y Funcionamiento de la Comisión de Adquisición de las Dirección Generales y Nacionales, de los Comandos Provinciales y Unidades Especiales de la Policía Nacional, aprobado y vigente por el mando policial.

DISPOSICION TRANSITORIA.-

Art. 26.- En virtud de lo establecido en la Ley Orgánica de la Policía Nacional y en el presente Reglamento de las Dirección Nacional de Comunicación, sustituyese la denominación de Departamento de Comunicación por Dirección Nacional de Comunicaciones, igualmente en cuanto a sus funciones y en todo lo que fuere necesario:
2.- Publicar la presente resolución en la Orden General de la Institución de acuerdo con el Art. 87 de la Ley Orgánica de la policía Nacional y Art. 43 del Reglamento del Consejo de Generales de la Policía Nacional.
Dado y firmado, en la sala de sesiones del Consejo de Generales de la Policía Nacional, en la ciudad de San Francisco de Quito, a los seis días del mes de septiembre del dos mil.
f) DR. MARIO ROMEL CEVALLOS MORENO.- GENERAL INSPECTOR.- PRESIDENTE DEL CONSEJO DE GENERALES DE LA POLICÍA NACIONAL.- f) ING. JORGE MOLINA NUÑEZ.- GENERAL INSPECTOR.- VOCAL DEL CONSEJO DE GENERALES DE LA POLICÍA NACIONAL.-f) DR. EDGAR VACA VINUEZA.- GENERAL DE DISTRITO.- VOCAL DEL CONSEJO DE GENERALES DE LA POLICÍA NACIONAL.- f) LIC. ENRIQUE VENEGAS PACHECO.- POLICIA NACIONAL.- f) DR. EDUARDO MONCAYO GALLEGOS.- CORONEL DE POLICA DE JUSTICIA.- DIRECTOR NACIONA DE ASESORÍA JURÍDICA DE LA POLICÍA NACIONAL.

1.4 PERSONAL DIRECTIVO

Está conformado por las siguientes personas los mismos que ocupan el respectivo cargo.

CARGO	NOMBRES	CEDULA
Director Nacional de Telecomunicaciones e Informática	Jara López Jaime Bladimir	170762733-5
Jefe de la División Redes	Naranjo Rubio Augusto Giovanni	050200265-2
Jefe de Operaciones	Piedra Ramírez Eduardo Favio	170897543-6
Jefe de Ingeniería	Almache Moreno Ruth Marina	170757071-7

2.1. SERVICIO QUE OFRECE LA INSTITUCIÓN

La División Redes presta los servicios que a continuación se detalla:

- ✓ Mantenimiento preventivo y correctivo de equipos de cómputo.
- ✓ Programación de equipos de comunicación.
- ✓ Administra los Centros de Proceso de Datos y la información de los Servicios Policiales, a través de grupos de trabajo dedicados;
- ✓ Proponer el diseño, montaje y operacionalización del Hardware requeridos por la Institución
- ✓ Administración de la "Red Troncalizado Nacional"
- ✓ Diseño y ejecución de proyectos tecnológicos de la Policía Nacional.
- ✓ Diseño, implementación y mantenimiento de sistemas de climatización, sistemas de respaldo de energía y sistemas de protección a tierra.
- ✓ Diseño y elaboración de programas informáticos.
- ✓ Asesoría técnica a las diferentes unidades policiales.

3.1. PRINCIPALES DEPARTAMENTOS DE LA DIVISIÓN REDES CON UNA BREVE INDICACIÓN DE SUS FUNCIONES Y NÚMERO DE PERSONAS QUE LOS CONFORMA

La División Redes desarrolla sus actividades funcionales con tres departamentos principales que se detallan, a continuación:

Departamento de operaciones.- Se encuentra dirigida por un oficial, con título profesional de tercer nivel, en la especialidad de Ing. Electrónica y Telecomunicaciones, cuenta con tres técnicos que poseen título profesional en Ing. Electrónica y Ing. Telecomunicaciones, los cuales se encargan de ofrecer asesoría tecnológica a las diferentes unidades policiales, además se encuentra dividido en dos secciones tales como la sección de Laboratorio y la sección de Asistencia Técnica.

Departamento de Ingeniería.- Se encuentra dirigida por un oficial, con título profesional de tercer nivel, en la especialidad de Ing. Electrónica, cuenta con tres técnicos que poseen título profesional en Ing. Sistemas, su principal función es brindar mantenimiento preventivo y correctivo de los equipos de comunicación, además se encuentra dividido en dos secciones tales como la sección de Mantenimiento Básico y la sección de Mantenimiento Avanzado.

Departamento de Administración del Sistema Troncalizado.- Se encuentra dirigida por el mismo oficial del departamento de operaciones, cuenta con cuatro personas que poseen título de tercer nivel en la especialidad de Ing. Telecomunicaciones, su función principal es administrar la red Troncalizado a nivel nacional.

3.2. DETALLE DE EQUIPOS INFORMÁTICOS QUE POSEE LA DIVISIÓN REDES

N°	Sección	Descripción	Serie	Marca	Características	Observaciones
1	Ingeniería	Computadora	2UA202061B	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado
2	Ingeniería	Computadora	2UA2151MS7	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado
3	Ingeniería	Computadora	2UA2151BXY	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 08-11-2012
REVISADO POR: L.F.P.	FECHA: 08-11-2012

N°	Sección	Descripción	Serie	Marca	Características	Observaciones
4	Ingeniería	Computadora	2UA202061L	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado
5	Operaciones	Computadora	2UA034004V	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado
6	Operaciones	Computadora	2UA2080V8H	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 08-11-2012
REVISADO POR: L.F.P.	FECHA: 08-11-2012

N°	Sección	Descripción	Serie	Marca	Características	Observaciones
7	Operaciones	Computadora	MXJ94706YJ	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado
8	operaciones	Computadora	2UA1450NMT	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado
9	Administración Sistema Troncalizado	Computadora	MXJ94706S6	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado

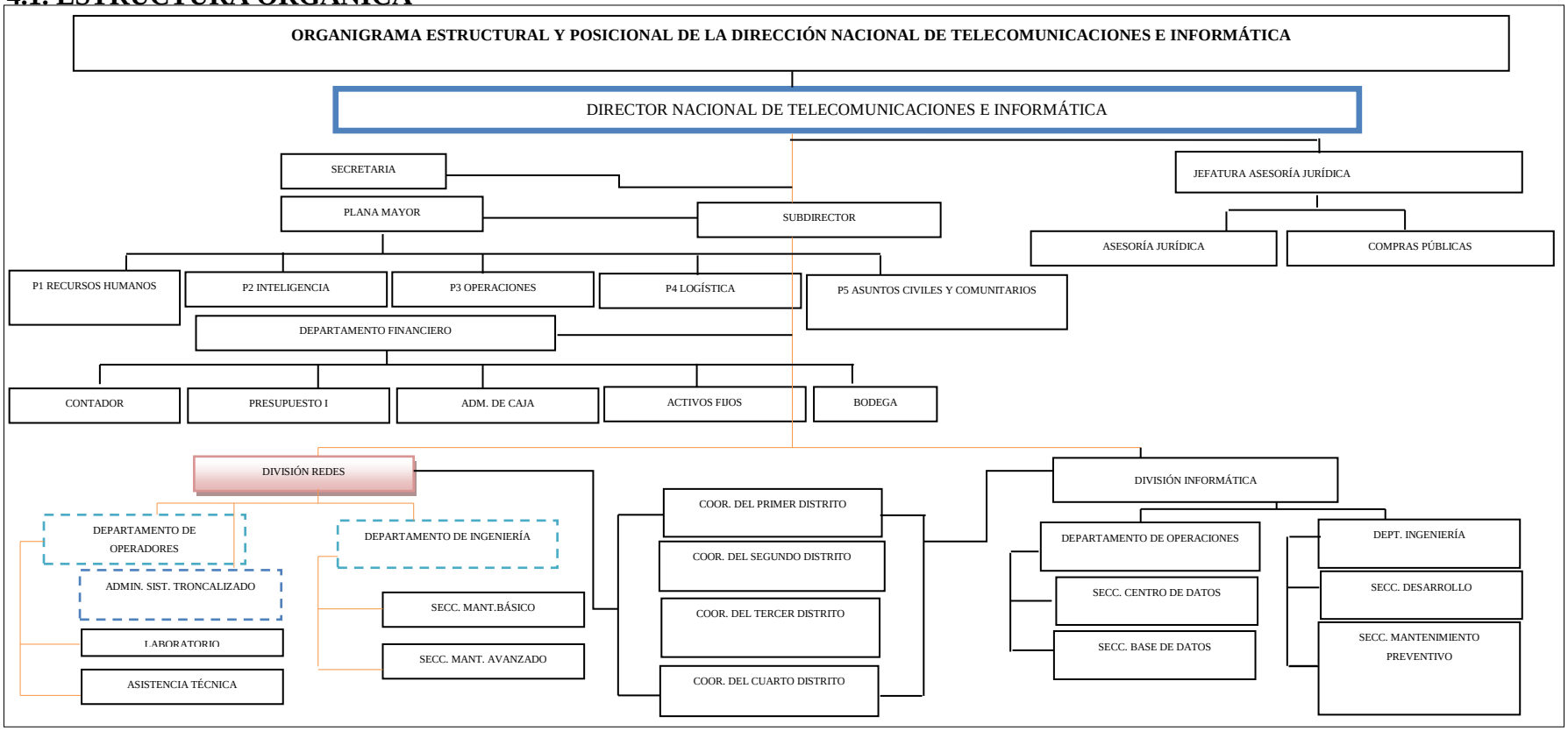
N°	Sección	Descripción	Serie	Marca	Características	Observaciones
10	Administración Sistema Troncalizado	Computadora	2UA040JSP	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado
11	Administración Sistema Troncalizado	Computadora	2UA0440K15	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado
12	Administración Sistema Troncalizado	Computadora	2UA2151MVO	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 08-11-2012
REVISADO POR: L.F.P.	FECHA: 08-11-2012

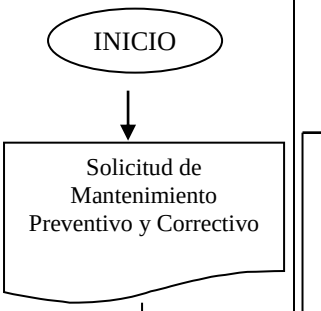
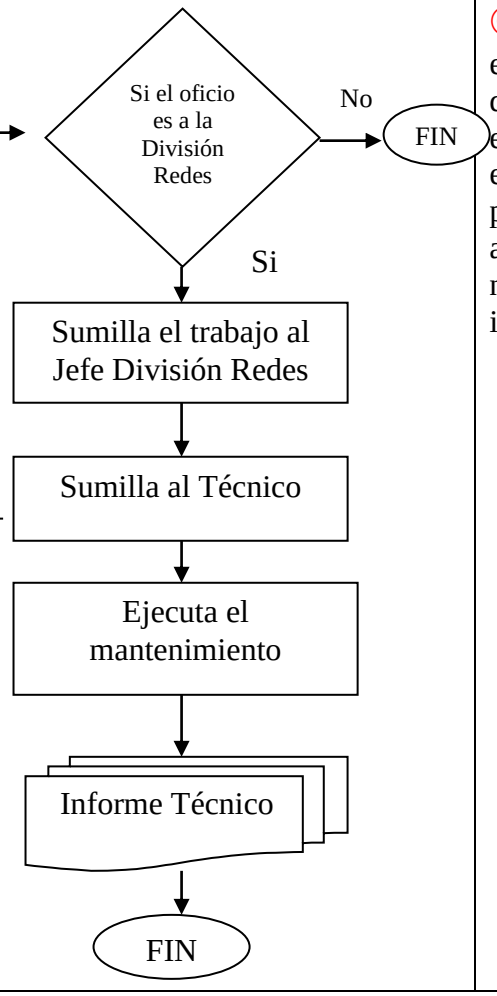
N°	Sección	Descripción	Serie	Marca	Características	Observaciones
13	Operaciones	Computadora	2UA202061V	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado
8	operaciones	Impresora laser	MXJ9470832	Hewlett-Packard	Impresora B/n, color alta resolución	Buen estado
9	Administración Sistema Troncalizado	Computadora Portatil	H8758M1	DELL	Memoria RAM: 4,00GHz Procesador Intel Core i3 de 2.2GHz Sistema Operativo: Windows VISTA Disco Duro: 500 GHz	Buen estado

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 08-11-2012
REVISADO POR: L.F.P.	FECHA: 08-11-2012

4.1. ESTRUCTURA ORGÁNICA

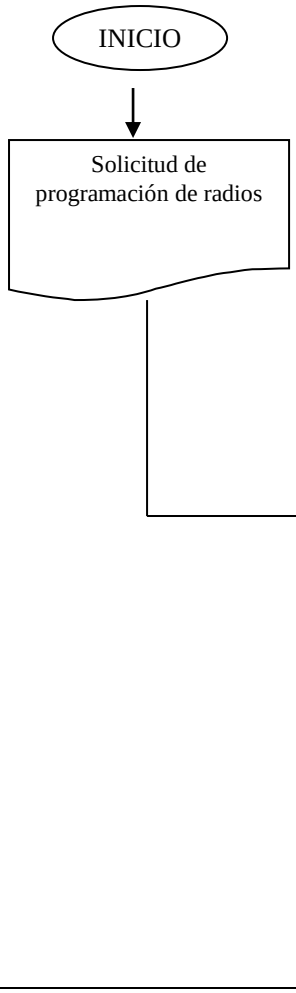
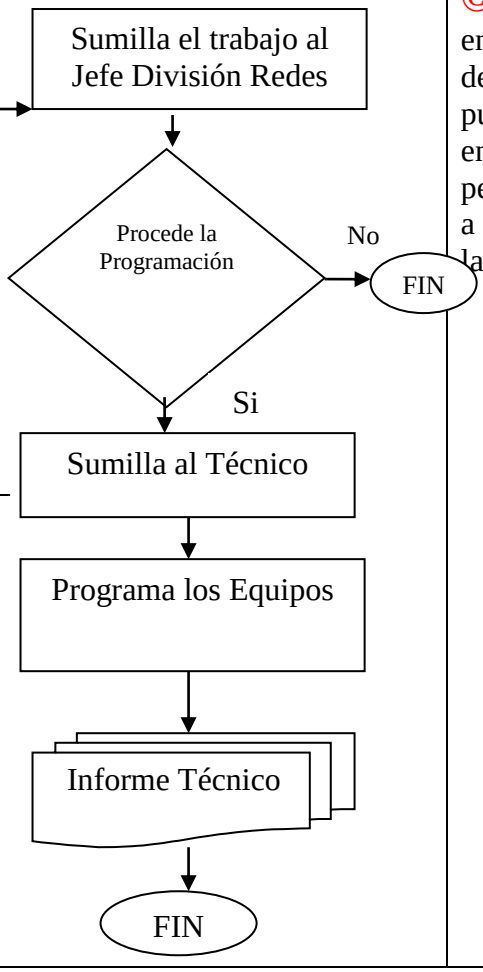


4.2. PROCESO DE MANTENIMIENTO DE EQUIPOS CÓMPUTO

UNIDAD QUE SOLICITA	DIRECCIÓN NACIONAL DE TELECOMUNICACIONES E INFORMÁTICA	COMENTARIO
		© El proceso se encuentra en forma detallada y desde el punto de vista se encuentra perfectamente, acorde a las necesidades de la institución.

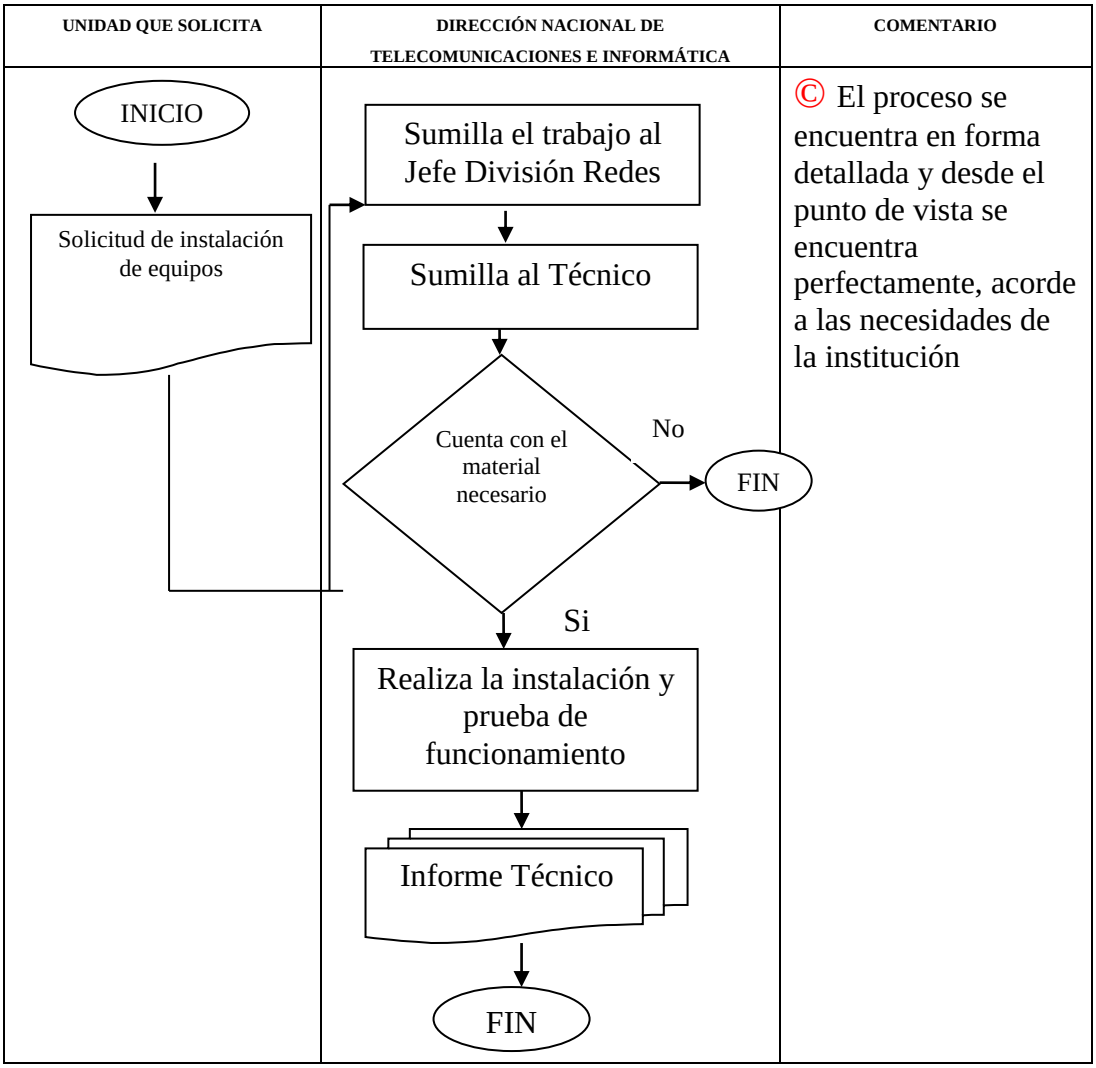
ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 12-11-2012
REVISADO POR: L.F.P.G	FECHA: 12-11-2012

4.3. PROCESO DE PROGRAMACIÓN DE EQUIPOS DE CÓMPUTO

UNIDAD QUE SOLICITA	DIRECCIÓN NACIONAL DE TELECOMUNICACIONES E INFORMÁTICA	COMENTARIO
		© El proceso se encuentra en forma detallada y desde el punto de vista se encuentra perfectamente, acorde a las necesidades de la institución

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 12-11-2012
REVISADO POR: L.F.P.G	FECHA: 12-11-2012

4.4. PROCESO DE INSTALACIÓN DE EQUIPOS TIPO BASE Y MÓVILES



ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 12-11-2012
REVISADO POR: L.F.P.G	FECHA: 12-11-2012

3.6 Archivo Corriente

3.6.1 Fase I Estudio Preliminar

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
FASE I ESTUDIO PRELIMINAR
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

F I

	CONTENIDO	**REF.**
	Programa de Auditoría	P/A 2/9
1.1	Formulario de Visita Previa	F/V.P 1/5
1.2	Carta de Presentación de la Firma Auditora	C/P 1/1
1.3	Propuesta de Servicios	P/S 1/1
1.4	Propuesta Técnica	P/T 1/5
1.5	Contrato de Servicios de Auditoría	C/S.A 1/3
1.6	Comunicación de inicio de examen	C/I.E 1/1
1.7	Cédula narrativa del cumplimiento de Seguridades	I/S 1/1
1.8	Informe de Cumplimiento de la Fase I	I/C 1/3

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 21-10-2012
REVISADO POR: L.F.P.G	FECHA: 21-10-2012

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
PROGRAMA DE AUDITORÍA
FASE I ESTUDIO PRELIMINAR
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

P/A 2/9

OBJETIVO

- ✓ Conocer a la institución estableciendo puntos críticos para efectuar el análisis correspondiente.

Nº	PROCEDIMIENTO	REF. P/T	ELABORADO POR:	
			AUDITOR	FECHA
1	Elaboración del cuestionario "Guía de Visita Previa" para la obtención de información haciendo constar preguntas para una evaluación preliminar de Control Interno.	F/V.P 1/5	Consulexter S.A	22-10-2012
2	Elaboración de la propuesta de servicios y Contrato de Auditoría	P/T 1/5 C/S.A 1/3	Consulexter S.A	29-10-2012 01-11-2012
3	Prepare comunicaciones de inicio de auditoría	C/I.E 1/1	Consulexter S.A	04-11-2012
4	Elabore una cédula narrativa con el resultado de cumplimiento de políticas y objetivos de seguridades implantadas.	I/S 1/2	Consulexter S.A	13-11-2012
5	Elaboración del informe de cumplimiento de la fase incluyendo los resultados obtenidos de la evaluación preliminar de control interno.	I/C 1/3	Consulexter S.A	16-11-2012

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 21-10-2012
REVISADO POR: L.F.P.G	FECHA: 21-10-2012

1.1 FORMULARIO DE VISITA PREVIA

INFORMACIÓN GENERAL:

Nombre de la Entidad: División Redes de la Dirección Nacional de Telecomunicaciones e Informática de la Policía Nacional

Dirección: Calle Rither Oe 9-141 y Diego Zorrila sector La Gasca

Teléfono:

Fecha de Creación de la Institución: 03 de octubre del 2000

Funciones Principales: Desarrollar las funciones de comunicaciones e informática, para apoyar todas las labores de la Policía Nacional a fin de optimizar la gestión institucional.

Alcance del examen: Del 1 de octubre del 2012 al 31 de enero del 2013

1. Ha sido evaluado la Seguridad Física de la División Redes:

SI [ ] NO [X]

Fecha:

2. ORGANIZACIÓN Y FUNCIONES

2.1. Se han definido los objetivos generales y específicos para la División Redes:

SI [ ] NO [X]

2.2. La estructura orgánica de la División Redes está definida:

SI [X] NO [ ]

2.3. Es adecuada la dependencia jerárquica actual.

SI [X] NO [ ]

Señale las causas:

2.4. Hay una definición clara de las funciones a nivel de cargo:

SI [ ] NO [X]

3. RECURSOS HUMANOS

3.1. Cuenta la División Redes con personal capacitado:

SI [X] NO [ ]

3.2. La formación profesional tiene relación con el trabajo que realizan.

SI [X] NO [ ]

4. DESARROLLO DE SISTEMAS

4.1. Cuáles son las unidades usuarias de la información de los diferentes sistemas.

Departamento de Operaciones

Departamento de Administración de la Red Troncalizada

Departamento de Ingeniería

4.2. ¿Existe una metodología escrita para el desarrollo de sistemas informáticos de forma Física?

No posee ningún manual que permita conocer los procedimientos para el desarrollo y utilización de los equipos e instalaciones eléctricas que mantiene la División Redes.

4.3. ¿Se protegen los equipos e instalaciones, se encuentran actualizadas?

En cuanto a los equipos se puede asumir que existe un grado de seguridad puesto que no se encuentran expuestos a humedad, y la División Redes se encuentra en una zona segura. Mientras que las instalaciones se encuentran bajo regletas pero no en su totalidad exponiéndose de tal manera a que sufran cortocircuitos o destrucción. La Edificación donde se encuentra ubicada la División Redes es de hormigón armado pero ya se está deteriorando sus paredes despiden mucho polvo debido a la falta de mantenimiento.

4.4. **Hardware**

¿Los equipos de cómputo son en?

Compra [X] **Arrendamiento** [ ] **Donación** [ ]

Marca: INTEL Modelo: 2011

Capacidad memoria real: 2GB

Memoria en discos: 750GB

Equipos Periféricos: Posee teclado, Mouse, Monitor

5.2 ¿Considera que los equipos de cómputo están totalmente utilizados?

SI [X] NO [ ]

5. CONTROL INTERNO

5.1. **¿Las instalaciones contemplan seguridades para prevención de incendios, robos, inundaciones y otros desastres?**

SI [X] NO [ ]

Observaciones: Se contempla ciertas seguridades como por ejemplo posee un sistema de alarma, sensores de humo, extintores, pero no posee letreros de señalización donde indique salidas de emergencia control de acceso.

5.2. **¿Está controlado el acceso al área del centro de datos?**

Si existe un control del acceso ya que cuenta con personal de guardianía las 24 horas del día.

5.3. **¿Está asegurado el equipo de Cómputo y las instalaciones?**

Todos los activos de la institución están asegurados pero los archivos se encuentran en la Comandancia General de la Policía Nacional.

5.4. **¿Se controla continuamente la temperatura, humedad, etc., de los equipos de cómputo?**

Si se controla dos veces por día

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 22-10-2012
REVISADO POR: L.F.P.G.	FECHA: 22-10-2012

5.5. ¿Existe un sistema de respaldo que garantice la provisión permanente de energía eléctrica?

No cuentan con una fuente de poder capaz de dar energía al computador cuando se suprime la corriente eléctrica,

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 22-10-2012
REVISADO POR: L.F.P.G.	FECHA: 22-10-2012

1.2 CARTA PRESENTACIÓN DE LA FIRMA AUDITORA

Quito, 29 de Octubre del 2012.

Crnl. Jaime Bladimir Jara López
DIRECTOR NACIONAL DE TELECOMUNICACIONES E INFORMÁTICA
Presente.-

De nuestra consideración:

Mediante la presente le extendemos un atento y cordial saludo; el motivo de esta carta es para presentarnos como Consulexter S.A., quienes prestamos servicios a nivel Nacional, de Auditoría: Externa, Tributaria, De Estados Financieros, Administrativa, Informática; con dirección en la ciudad de Latacunga Barrio San Felipe, calle Eloy Alfaro Nº 1030, dicha asociación está conformada por Susana Bastidas y Ana Calero, quienes necesitan realizar ésta práctica como último requisito para la obtención del Título de Ingeniaría en Contabilidad y Auditaría.

Por la favorable atención agradecemos la aceptación de nuestros servicios dentro la institución.

Atentamente,

Susana Bastidas Egresada. C.I: 172217134-3	Ana Calero Egresada. C.I: 050359487-1

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 29/10/2012
REVISADO POR: L.F.P.G.	FECHA: 29/10/2012

1.3 PROPUESTA DE SERVICIOS

Quito, 29 de Octubre del 2012.

Crnl. Jaime Bladimir Jara López
DIRECTOR NACIONAL DE TELECOMUNICACIONES E INFORMÁTICA
Presente.-

De nuestras consideraciones:
La División Redes, representada por el Crnl. Jaime Jara Director Nacional de Telecomunicaciones e Informática autoriza realizar la Auditoría a la Seguridad Física para el departamento, en el período correspondiente al 1 de octubre del 2012 al 31 de enero del 2013; a Consulexter S.A., conformado por las señoritas: Susana Bastidas y Ana Calero, con el fin de realizar el trabajo investigativo previo a la obtención del Título de Ingenieras en Contabilidad y Auditoría.

A continuación ponemos a vuestra consideración la propuesta de trabajo.

Por la favorable atención que se digne dar a la presente anticipamos nuestros más sinceros agradecimientos.

Atentamente

Susana Bastidas
Egresada.
C.I: 172217134-3

Ana Calero
Egresada.
C.I: 050359487-1

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 29/10/2012
REVISADO POR: L.F.P.G	FECHA: 29/10/2012

1.4 PROPUESTA TÉCNICA

NATURALEZA DEL ESTUDIO:

Auditoría a la Seguridad Física

ALCANCE:

La Auditoría a la Seguridad Física, se realizará en la Dirección Nacional de Telecomunicaciones e Informática "División Redes" y cubrirá el periodo comprendido entre el 1 de octubre del 2012 al 31 de enero del 2013 y se examinará los aspectos de seguridades físicas, procedimientos, documentación y utilización del hardware.

CAMPO DE APLICACIÓN:

Determinar la integridad de los recursos humanos, equipos, y materiales de la institución.

OBJETIVO:

Contribuir al desarrollo de revisión de los recursos informáticos en la División Redes de la Dirección Nacional de Telecomunicaciones e Informática, así como la verificación de lo físico, lo funcional y lo humano.

CONTROL INTERNO:

Se evaluará a través de cuestionarios de Auditoría a la Seguridad Física los cuales contienen características y cualidades de la División Redes.

PERÍODO A REVISAR:

Del 1 de octubre del 2012 al 31 de enero del 2013

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 29/10/2012
REVISADO POR: L.F.P.G.	FECHA: 29/10/2012

ESTRATEGIAS:

Observación de las instalaciones, cumplimiento de normas.

Revisión de los procedimientos de seguridad física; contratos de seguro y mantenimiento.

Aplicar instrumentos de investigación.

Establecer recomendaciones específicas para el elemento bajo revisión.

ACCIONES:

Aplicación de entrevistas, encuestas y la observación da campo

RECURSOS: HUMANOS:

Srta. Susana Bastidas

Srta. Ana Calero

RECURSOS MATERIALES:

Flash Memory

Suministros y materiales de oficina, otros

RECURSOS FINANCIEROS:

- Transporte, alimentación
- Imprevistos

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 29/10/2012
REVISADO POR: L.F.P.	FECHA: 29/10/2012

RESULTADO ESPERADO:

Emitir un informe que contenga las guías necesarias para la evaluación independiente de los recursos humanos, equipos y materiales; sintetizando riesgos, deficiencias, sugerencias y recomendaciones.

INFORMACIÓN COMPLEMENTARIA:

Recopilación y revisión de todo el material normativo, administrativo, y funcional de la institución.

Con el propósito de obtener toda la colaboración por parte del personal del área objeto de examen, se les ha informado que se efectuará una Auditoría a la Seguridad Física en las fechas programadas.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 29/10/2012
REVISADO POR: L.F.P.G.	FECHA: 29/10/2012

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
FASE I ESTUDIO PRELIMINAR
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

P/T 4/5

CURRICULUM VITAE

Cargo propuesto: Auditor Jefe
Nombre de la firma: Consulexter S.A.

DATOS PERSONALES

Nombres: Susana Mercedes
Apellidos: Bastidas Bonilla
Fecha de nacimiento: 28 de Agosto de 1987
Cedula de Identidad: 172217134-3
Nacionalidad: Ecuatoriana
Teléfono: 0983874469

FORMACIÓN ACADÉMICA

SUPERIOR: Universidad Técnica de Cotopaxi
- ✓ Egresada en Ing. Contabilidad y Auditoría. CPA

SECUNDARIA: Colegio Nacional Técnico Simón Bolívar
- ✓ Título: Contadora Bachiller en Ciencias de Comercio y Administración

SUFICIENCIA EN INGLES
- ✓ Universidad Técnica de Cotopaxi

CURSOS REALIZADOS
- ✓ Educación y Capacitación Tributaria
- ✓ Seminario de Declaraciones de Impuestos

CONOCIMIENTO BÁSICOS
- ✓ Microsoft Office, Mónica 7, Internet, Declaración de impuesto, Elaboración de Contabilidades, IEES

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 29/10/2012
REVISADO POR: L.F.P.G.	FECHA: 29/10/2012

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
FASE I ESTUDIO PRELIMINAR
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

P/T 5/5

CURRICULUM VITAE

Cargo propuesto: Auditor Señor
Nombre de la firma: Consulexter S.A.

DATOS PERSONALES

Nombre del individuo: Ana Rocío Calero Yánez
Fecha de nacimiento: 20 de Diciembre 1889
Cedula de Identidad: 050359487-1
Nacionalidad: Ecuatoriana
Teléfono: 0959795134

FORMACIÓN ACADÉMICA

SUPERIOR: Universidad Técnica de Cotopaxi

- ✓ Egresada en Ing. Contabilidad y Auditoría. CPA

SECUNDARIA: Colegio Técnico Pujilí

- ✓ Bachiller Técnico Administración y Contabilidad

SUFICIENCIA EN KICHUA

- ✓ Universidad Técnica de Cotopaxi

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 29/10/2012
REVISADO POR: L.F.P.G.	FECHA: 29/10/2012

1.5 CONTRATO DE SERVICIOS DE AUDITORÍA

Quito, 01 de Noviembre del 2012

En la Provincia de Pichincha Cantón Quito Parroquia Quito Calle Rither Oe 9-141 y Diego Zorrila sector La Gasca se celebra el contrato de Auditoría entre el Crnl. Jaime Bladimir Jara López Director Nacional de Telecomunicaciones e Informática de la Policía Nacional y la Representante Legal de la Firma Consulexter S.A., Ing. Bastidas Bonilla Susana Mercedes en cuyo contrato se especifican los derechos y obligaciones de las partes.

CLÁUSULA PRIMERA.- OBJETIVO

El auditor se obliga a prestar al cliente los servicios de Auditoría Informática a la Seguridad Física para llevar a cabo la evaluación de seguridades físicas de los equipos, instalaciones y del personal del cliente, que se detalla en la propuesta de servicios anexa que, firmada por las partes, forma parte integrante del contrato.

CLÁUSULA SEGUNDA.- ALCANCE DEL TRABAJO

El alcance de los trabajos que llevara a cabo el auditor dentro de este contrato son:

- ✓ Evaluaciones de la dirección de seguridades físicas de los equipos, instalaciones y del personal en lo que corresponde a:
  - ✓ Su organización -capacitación
  - ✓ Estructura -planes de trabajo
  - ✓ Recursos humanos -controles
  - ✓ Normas y políticas –estándares
  - ✓ Evaluación de los diferentes sistemas en operación, (flujo de información, procedimientos, documentación, redundancia, organización de archivos, estándares de programación, controles, utilización de los sistemas).
  - ✓ Evaluación de prioridades y recursos asignados (humanos y equipo de cómputo).

- ✓ Evaluación de equipos
  - ✓ Capacidades -respaldos de equipo
  - ✓ Utilización -seguros
  - ✓ Nuevos proyectos -contratos
- ✓ Elaboración de un informe que contenga conclusiones y recomendaciones por cada uno de los trabajos señalados en esta cláusula.

CLÁUSULA TERCERA. PROGRAMA DE TRABAJO

El cliente y el auditor convienen en desarrollar en forma conjunta un programa de trabajo en el que se determinen con precisión las actividades a realizar por cada una de las partes, los responsables de llevarlas a cabo y las fechas de realización.

CLÁUSULA CUARTA.- RELACIÓN LABORAL

El personal del auditor no tendrá ninguna relación laboral con el cliente y queda expresamente estipulado que este contrato se suscribe en atención a que el auditor en ningún momento se considera intermediario del cliente respecto al personal que ocupe para dar cumplimiento de las obligaciones que se deriven de la relaciones entre él y su personal, y exime al cliente de cualquier responsabilidad que a este respecto existiere.

CLÁUSULA QUINTA.- PLAZO DE TRABAJO

El auditor se obliga a terminar los trabajos señalados en la cláusula segunda de este contrato en 70 días hábiles después de la fecha en que se firme el contrato. El tiempo estimado para la terminación de los trabajos esta en relación a la oportunidad en que el cliente entregue los documentos requeridos por el auditor y por el cumplimiento de las fechas estipuladas en el programa de trabajo aprobado por las partes, por lo que cualquier retraso ocasionado por parte del personal del cliente o de usuarios de los sistemas repercutirá en el plazo estipulado, el cual deberá incrementarse de acuerdo a las nuevas fechas establecidas en el programa de trabajo, sin perjuicio alguno para el auditor.

CLÁUSULA SEXTA.- HONORARIOS

Debido a que la Auditoría Informática a la Seguridad Física corresponde a un trabajo de investigación, no tendrá ningún costo los gastos y honorarios en que se incurrirá serán asumidos en su totalidad por la firma Auditora.

CLÁSULA SÉPTIMA.- CAUSAS DE RESCISIÓN

Serán causas de rescisión del presente contrato la violación o incumplimiento de cualquiera de las cláusulas de este contrato.

CLÁUSULA OCTAVA.- DOMICILIO:

Para todos los efectos de este contrato las partes convienen en fijar su domicilio del CONTRATANTE Quito, calle Rither Oe 9-141 y Diego Zorrila sector La Gasca AUDITORA, en la ciudad de Latacunga Barrio San Felipe, Calle Eloy Alfaro Nº 1030.

Enteradas las partes del contenido y alcance legal de este contrato, lo rubrican y firman de conformidad en original y tres copias en la ciudad de Quito, el día 01 de Noviembre del 2012.

Egda. Susana Bastidas
Nombre y firma del Representante Legal de la firma

Crnl. Jaime Bladimir Jara López
Nombre y firma del Representante Legal de la Dirección Nacional de Telecomunicaciones e Informática

Dr.
Notario Segundo de Pichincha

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 01-11-2012
REVISADO POR: L.F.P.G.	FECHA: 01-11-2012

1.6 COMUNICACIÓN DE INICIO DE EXAMEN

PARA: Crnl. Ing. Jaime Bladimir Jara López
DIRECTOR NACIONAL DE TELECOMUNICACIONES E INFORMÁTICA
DE: JEFE DE AUDITORÍA
ASUNTO: Comunicación inicio de examen
FECHA: 04 de Noviembre de 2012

Cúmpleme comunicarle que la Dirección de Auditoría Externa dio inicio a la Auditoría de la Seguridad Física en la División Redes, el 31 de Octubre del 2012, por el periodo comprendido entre el 1 de octubre del 2012 al 31 de enero del 2013 .

Con esta oportunidad agradeceré remitir a la Dirección de Auditoría Externa, ubicada en la en la ciudad de Latacunga Barrio San Felipe, calle Eloy Alfaro Nº 1030, cualquier documentación que tenga relación con el examen relacionado y prestar toda colaboración necesaria a fin de que los resultados logrados sean de beneficio para la institución.

Egda. Susana Bastidas
JEFE DE AUDITORÍA

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 04-11-2012
REVISADO POR: L.F.P.	FECHA: 04-11-2012

1.7 CUMPLIMIENTO DE SEGURIDADES

El principal objetivo es obtener información previa del estado de la institución, esto ayuda a generar horizontes que guíen a la determinación de la conveniencia de seguir o no con el ejercicio de la auditoría. Una de las razones es la ausencia de auditorías, puesto que cuando se aplicó el formulario de guía de visita previa se pudo determinar que en esta institución no se había realizado ninguna clase de auditoría.

Aplicando la técnica de verificación ocular, se logró verificar el buen estado físico de los equipos, su operatividad, el número de equipos que poseen que en su total cuentan con 13 computadores de escritorio y 1 computadoras portátil, existiendo una adecuada distribución de equipos, cumpliendo así con la norma 400-11 con título: Aprovechamiento de los recurso computarizados.

Al aplicar la técnica revisión selectiva, se comprobó que no existe documento alguno de establecimiento de políticas internas de la División Redes donde se ponga en manifiesto la segregación de funciones específicas, además no cuentas con un Plan de Contingencia que ayude a salvaguardar los equipos y al personal en caso de un desastre.

El personal que labora en la División Redes está capacitado ya que en su mayoría cuentan con título profesional de tercer nivel en telecomunicaciones y electrónica, además reciben capacitaciones constantes tanto nacional e internacionalmente como por ejemplo en programación de equipos, en Estados Unidos. Cumpliendo así con el plan de actividades programado por la Institución.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 13-11-2012
REVISADO POR: L.F.P.G	FECHA: 13-11-2012

Luego de este análisis se puede concluir que la ejecución de Auditoría a la Seguridad Físicas es conveniente continuar puesto que en el desarrollo de la fase preliminar se hallaron acierto y errores que ameritan la investigación más profunda de los mismos.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 13-11-2012
REVISADO POR: L.F.P.G	FECHA: 13-11-2012

1.8 INFORME DE CUMPLIMIENTO DE LA FASE I

Como primer paso se elaboró la propuesta de servicio para posteriormente llevar a cobo la redacción del contrato de Auditoría en el cual se hizo constar el tiempo en el que se llevará a cabo dicha Auditoría.

En segundo lugar se presentó comunicados de inicio de examen, en el que se hizo constar la fecha de inicio así como el periodo comprendido para dicho examen, de este modo todos los involucrados tuvieron conocimiento y colaboraron en la ejecución del trabajo.

Otra de las tareas cumplidas fue la aplicación de un formulario denominado Guía de Visita Previa en el cual se obtuvo información general sobre control interno, políticas, recursos que disponen, etc.

Otra tarea cumplida es la obtención y elaboración de organigramas estructurales, flujogramas de los diferentes procesos, se elaboró un croquis donde se puede ubicar geográficamente al edificio de la División Redes y se solicitó más documentación que ayudó a evaluar el cumplimiento de las seguridades dentro la institución.

Con la obtención de estos datos hemos podido tener una visión de qué tipo de organización es la que vamos a examinar y poder realizar un análisis previo de los aspectos que deberemos tomar en cuenta para la ejecución a futuro.

3.6.2 Fase II Revisión y Evaluación de Controles y Seguridades

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
ÍNDICE FASE II REVISIÓN Y EVALUACIÓN DE CONTROLES Y SEGURIDADES
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

F II

	CONTENIDO	REF.
	Programa de Auditoría	P/A 3/9
1.1	Memorándum de Planificación Estratégica	M/P 1/4
1.2	Conocimiento del entorno	C/E 1/1
1.3	Definición de componentes	D/C 1/1
1.4	Cuestionarios de Control Interno por componente	C/C.I 1/6
1.5	Matriz de evaluación preliminar de riesgo	M/E.C 1/9
1.6	Informe sobre la evaluación de la estructura del Control Interno	I/C 2/3

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 19-11-2012
REVISADO POR: L.F.P.G	FECHA: 19-11-2012

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
PROGRAMA DE AUDITORÍA
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

P/A 3/9

OBJETIVO

Evaluar el Sistema de Control Interno, el cual permite evaluar los sistemas de información y los procedimientos de seguridades de cada componente.

Nº	PROCEDIMIENTO	REF. P/T	ELABORADO POR:	
			AUDITOR	FECHA
1	Elabore el Memorándum de Planificación Estratégica.	M/P 1/4	Consulexter S.A	20-11-2012
2	Determinar las fortalezas, debilidades, oportunidades y amenazas a través del análisis FODA	C/E 1/1	Consulexter S.A	21-11-2012
3	Desarrolle y aplique el cuestionario de control interno para los componentes determinados: -Edificio -Instalaciones -Equipos de Computo -Personal	C/C.I 1/6	Consulexter S.A	27/11/2012
4	Califique y determine el nivel de riesgo por cada uno de los componentes que posee la División Redes.	M/E.C 1/9	Consulexter S.A	03-12-2012
5	Elabore el informe de cumplimiento de la fase incluyendo los resultados obtenidos de la evaluación preliminar del Control interno.	I/C 2/3	Consulexter S.A	07-12-2012

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 19-11-2012
REVISADO POR: L.F.P.G	FECHA: 19-11-2012

1.1 MEMORANDUM DE PLANIFICACIÓN ESTRATÉGICA

ANTECEDENTES

Por medio de un oficio dirigido al Mayor de Policía Augusto Giovanni Naranjo Rubio, Jefe de la División Redes de la Dirección Nacional de Telecomunicaciones e Informática de la Policía Nacional, en el cual se pidió autorizar la ejecución de una Auditoría Informática a la Seguridad Física como requisito de grado y a su vez nuestra firma auditora Consulexter S.A., presento en días anteriores la propuesta de servicios, misma que fue aprobada por parte de la Institución con el objeto de que nuestra firma realice un informe en donde refleje todas las debilidades y fortalezas con las que cuentan, en tal virtud se procedió a la firma del contrato entre las partes, con ello la elaboración, presentación de las actividades que se van a desarrollar para poder auditar los equipos e instalaciones que pertenecen a la institución.

En tanto se ha iniciado la elaboración de los archivos correspondientes para poder realizar de una manera organizada la ejecución de la Auditoría, procediendo la institución a facilitarnos la documentación requerida para dar inicio al proceso.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 20-11-2012
REVISADO POR: L.F.P.G.	FECHA: 20-11-2012

OBJETIVOS DE LA AUDITORÍA

- ✓ Establecer el grado de eficiencia, efectividad y economía de los equipos e instalaciones implantados en la División Redes.
- ✓ Evaluar el sistema de control interno y seguridades implantadas en el área.
- ✓ Conocer la capacidad profesional que tienen cada uno de los miembros que laboran en la institución.
- ✓ Analizar si se da el debido uso a cada recurso que mantiene la División Redes.

ALCANCE DE LA AUDITORÍA

La Auditoría a la Seguridad Física, se realizará en la Dirección Nacional de Telecomunicaciones e Informática "División Redes" y cubrirá el periodo comprendido entre el 01 de octubre del 2012 al 31 de enero del 2013 y se examinará los aspectos de seguridades físicas, procedimientos, documentación y utilización del hardware.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 20-11-2012
REVISADO POR: L.F.P.G.	FECHA: 20-11-2012

DESCRIPCIÓN DE LA ENTIDAD

La Ley Orgánica de la Policía Nacional en su Art. 53 del año 1998, crea la Dirección Nacional de Comunicaciones, y mediante RESOLUCION No.2000-353-CG-PN del 3 de Octubre del 2000, aprueba y expide el Reglamento Orgánico - Funcional de la Dirección Nacional de Comunicaciones de la Policía Nacional.

ORGANIZACIÓN ETRUCTURAL

La División Redes está formada por el Departamento de Operaciones, Administración del Sistema Troncalizado y el Departamento de ingeniería.

FUNCIONES BÁSICAS

Programación, mantenimiento, administración y control de las actividades relacionadas con los equipos de cómputo y de comunicación de la Policía Nacional.

TIEMPO ESTIMADO

La Auditoría se pretende realizar en un tiempo estimado de tres meses comprendidos en 70 días laborables con un estimado de 5 horas de trabajo diarias los mismos que son cubiertos por la planificación correspondiente.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 20-11-2012
REVISADO POR: L.F.P.G.	FECHA: 20-11-2012

METODOLOGÍA DEL TRABAJO DE AUDITORÍA

Cada integrante del grupo de trabajo presentará al jefe de equipo los papeles de trabajo debidamente referenciados y archivados, además se mantendrá reuniones quincenales para hacer evaluaciones del avance del trabajo y para solucionar problemas presentados.

DISTRIBUCIÓN DEL INFORME

El informe definitivo se distribuirá de la siguiente manera

- ✓ Una copia para el Director Nacional de Telecomunicaciones e Informática
- ✓ Una copia para el Jefe de la División Redes
- ✓ Una copia para el Departamento Legal

FIRMA

…….

Consulexter S.A
Egda. Susana Bastidas
JEFE DE AUDITORÍA

.

……

Ing. Patricia López
SUPERVISOR

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 20-11-2012
REVISADO POR: L.F.P.G.	FECHA: 20-11-2012

1.2 CONOCIMIENTO DEL ENTORNO

FORTALEZAS	DEBILIDADES
✓ Trabajo en equipo. ✓ Buen trato al usuario interno y externo ✓ Personal capacitado ✓ Tecnología de punta ✓ Servicio de internet adecuado	✓ Cambio de mandos policiales. ✓ Infraestructura inadecuada. ✓ Carencia de un Plan Estratégico ✓ Falta de control de los Activos Fijos ✓ Carencia de un Plan de Contingencia ✓ Falta de coordinación y toma de decisiones.
OPORTUNIDADES	**AMENAZAS**
✓ Desarrollo Tecnológico ✓ Apoyo Gubernamental a través del Ministerio del Interior. ✓ Convenios y alianzas estratégicas con el Sector Público y Privado a nivel nacional e internacional. (CNT y Motorola). ✓ Buena ubicación geográfica	✓ Inestabilidad Política ✓ Virus ✓ Pérdida de información ✓ Cortes de energía eléctrica

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 21-11-2012
REVISADO POR: L.F.P.G.	FECHA: 21-11-2012

1.3 DEFINICIÓN DE COMPONENTES

Los componentes que se detalla a continuación facilitará el trabajo de la Auditoría por cuanto se obtendrá información concreta y correcta.

Edificio.- La infraestructura es de un solo piso, no cuenta con ventilación, las paredes se encuentra en mal estado debido la falta de mantenimiento.

Instalaciones.- Las instalaciones eléctricas se encuentran a simple vista, además no cuentan con una fuente de poder capaz de dar energía al computador cuando se suprime la corriente eléctrica.

Equipo de Cómputo.- El mantenimiento a los equipos de cómputo se lo realiza únicamente una vez al año, además no cuentan con un registro de inventario de los equipos.

Personal.- Cuenta con personas que tienen título profesional en las especialidades de Electrónica y Telemática, en la División Redes carecen de personal ya que laboran 13 personas incluidos los jefes departamentales, mismos que no son suficientes para cubrir con la demanda de servicios que presta a nivel nacional, además existen conflictos debido a que no existe separación de sus funcione y responsabilidades.

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
FASE II REVISIÓN Y EVALUACIÓN DE CONTROLES Y SEGURIDADES
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

C/C.I 1/6

CUESTIONARIO DE CONTROL INTERNO

SEGURIDADES EDIFICIO

	PREGUNTA	SI	NO	N/A	OBSERVACIONES
1	¿Se tiene materiales o paredes inflamables dentro del centro de cómputo?		X		
2	¿Se tiene grandes ventanas orientadas a la entrada o salida del sol?	X			
3	¿Se tiene paredes que despiden polvo?	X			
4	¿Existe alarmas para detectar (calor o humo) en forma automática?	X			
5	¿El techo y suelo del centro de cómputo esta hecho de algún material inflamable?	X			
6	¿Las puertas del centro de cómputo se cierran solas mediante algún mecanismo?	X			
7	¿Existe salida de emergencia?		X		
8	¿Existe en la División Redes un extinguidor de incendios?	X			
9	¿Cuenta la División Redes con equipo de aire acondicionado adecuado?		X		
10	¿Las pinturas de las paredes son de agua lavable?	X			

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 27-11-2012
REVISADO POR: L.F.P.G	FECHA: 27-11-2012

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
FASE II REVISIÓN Y EVALUACIÓN DE CONTROLES Y SEGURIDADES
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

C/C.I 2/6

CUESTIONARIO DE CONTROL INTERNO SEGURIDADES EN INSTALACIONES					
	PREGUNTA	**SI**	**NO**	**N/A**	**OBSERVACIONES**
1	¿El cableado se encuentra debidamente instalado en la División Redes?	X			
2	¿Los cables se encuentran debidamente identificado (positivo, negativo, tierra física)?	X			Código de colores(verde tierra, negro fase, otro color neutro)
3	¿Se cuenta con los planos de instalaciones eléctricas actualizados?	X			
4	¿Se tiene instalaciones eléctricas de equipo de cómputo independiente de otras instalaciones eléctricas?	X			
5	¿Se tiene reguladores para los equipos de cómputo?	X			Los CPS de 24 kva
6	¿Existe tableros de distribución eléctrica?	X			
7	¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlo?	X			

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 27-11-2012
REVISADO POR: L.F.P.G	FECHA: 27-11-2012

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
FASE II REVISIÓN Y EVALUACIÓN DE CONTROLES Y SEGURIDADES
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

C/C.I 3/6

CUESTIONARIO DE CONTROL INTERNO SEGURIDADES EN INSTALACIONES					
	PREGUNTA	**SI**	**NO**	**N/A**	**OBSERVACIONES**
8	¿Cuenta la División Redes con una fuente de poder capaz de dar energía al computador cuando se suprime la corriente eléctrica?	X			
9	¿La instalación eléctrica de la División Redes tiene conexión con la tierra?	X			
10	¿Si existe un estudio de carga del consumo de los equipos que están instalados?		X		No porque los equipos se instalaron en diferentes proyecto

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 27-11-2012
REVIDADO POR: L.F.P.G	FECHA: 27-11-2012

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
FASE II REVISIÓN Y EVALUACIÓN DE CONTROLES Y SEGURIDADES
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

C/C.I 4/6

CUESTIONARIO DE CONTROL INTERNO SEGURIDADES EQUIPO DE CÓMPUTO					
	PREGUNTA	**SI**	**NO**	**N/A**	**OBSERVACIONES**
1	¿Se tiene inventarios actualizados de los equipos y terminales con su localización?	X			
2	¿Se tiene seguros sobre todos los equipos que posee la División Redes?	X			
3	¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo?		X		Solo para aire acondicionado, generadores, equipos de computación
4	¿Si algún equipo ya es obsoleto, o no se está utilizando existe algún procedimiento para sustituir con un nuevo equipo?	X			Por medio de un informe técnico el encargado de activo fijo da de baja el equipo.
5	¿Existe un lugar suficiente para todos los equipos que dispone la División Redes?		X		Comparten espacios con los equipos de la División Informática.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 27-11-2012
REVISADO POR: L.F.P.G	FECHA: 27-11-2012

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
FASE II REVISIÓN Y EVALUACIÓN DE CONTROLES Y SEGURIDADES
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

C/C.I 5/6

CUESTIONARIO DE CONTROL INTERNO SEGURIDADES EQUIPO DE CÓMPUTO					
	PREGUNTA	**SI**	**NO**	**N/A**	**OBSERVACIONES**
6	¿Qué topología de Red utilizan las computadoras de la División Redes?	X			Topología en estrella concentrada en un swich
7	¿El gabinete que resguarda al RACK cuenta con ventiladores?	X			
8	¿Los cables de transmisión de datos son certificados y debidamente etiquetados?		X		No disponen con el equipo certificador de cables

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 27-11-2012
REVISADO POR: L.F.P.G	FECHA: 27-11-2012

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
FASE II REVISIÓN Y EVALUACIÓN DE CONTROLES Y SEGURIDADES
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

C/C.I 6/6

CUESTIONARIO DE CONTROL INTERNO
SEGURIDADES PARA EL PERSONAL

	PREGUNTA	SI	NO	N/A	OBSERVACIÓN
1	¿Existe una persona responsables de la seguridad en la División Redes?	X			Guardia
2	¿Es reconocido el trabajo fuera de horarios al personal?		X		
3	¿Se identifica a las personas que ingresa a la División Redes?	X			Registro en Libro diario de asistencias
4	¿Existe algún indicador de que está prohibido fumar?	X			
5	¿Realizan capacitaciones al personal que está laborando dentro de la División Redes?	X			Capacitaciones continúas dentro y fuera del país. 30 días cada año.
6	¿Existen políticas de vacaciones obligatorias al personal de la División Redes?	X			
7	¿Existe separación de funciones y de responsabilidades en la División Redes?		X		
8	¿Existe política para mantener la seguridad cuando termina la relación laboral con un empleado?	X			

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 27-11-2012
REVISADO POR: L.F.P.G	FECHA: 27-11-2012

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
FASE II REVISIÓN Y EVALUACIÓN DE CONTROLES Y SEGURIDADES
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

M/E.C 1/9

MATRIZ DE EVALUACIÓN DE CONTROL INTERNO SEGURIDADES EDIFICIO				
	PREGUNTA	**Pon**	**Calif**	**Responsable**
1	¿Se tiene materiales o paredes inflamables dentro del centro de cómputo?	10	8	Jefe de la D.R.
2	¿Se tiene grandes ventanas orientadas a la entrada o salida del sol?	10	7	
3	¿Se tiene paredes que despiden polvo?	10	4	
4	¿Existe alarmas para detectar (calor o humo) en forma automática?	10	6	
5	¿El techo y suelo del centro de cómputo esta hecho de algún material inflamable?	10	8	
6	¿Las puertas del centro de cómputo se cierran solas mediante algún mecanismo?	10	6	
7	¿Existe salida de emergencia?	10	9	
8	¿Existe en la División Redes un extinguidor de incendios?	10	8	
9	¿Cuenta la División Redes con equipo de aire acondicionado adecuado?	10	6	
10	¿Las pinturas de las paredes son de agua lavable?	10	4	
	TOTAL	**100**	**66**	

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 03-12-2012
REVISADO POR: L.F.P.G	FECHA: 03-12-2012

DETERMINACIÓN DEL RIESGO SEGURIDADES EDIFICIO

NC = CT/PT
NC = 66/ 100 = 0.66 X 100 = 66 **%**

RIESGO DE CONTROL

ALTO	MODERADO	BAJO
15.50%	51.75%	76.95%
BAJO	**MODERADO**	**ALTO**

NIVEL DE CONFIANZA

Conclusión: Como se pudo apreciar hemos obtenido una calificación de riesgo de 66% que nos da un nivel de confianza moderado con un riesgo moderado, de modo que la División Redes casi no tendría problemas con su edificio en caso de que ocurriera alguna desastre natural.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 03-12-2012
REVISADO POR: L.F.P.G	FECHA: 03-12-2012

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
FASE II REVISIÓN Y EVALUACIÓN DE CONTROLES Y SEGURIDADES
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

M/E.C 3/9

MATRIZ DE EVALUACIÓN DE CONTROL INTERNO SEGURIDADES EN INSTALACIONES				
	PREGUNTA	**Pon.**	**Calif.**	**Responsable**
1	¿El cableado se encuentra debidamente instalado en la División Redes?	10	9	Técnicos de la D.R
2	¿Los cables se encuentran debidamente identificado (positivo, negativo, tierra física)?	10	8	
3	¿Se cuenta con los planos de instalaciones eléctricas actualizados?	10	4	
4	¿Se tiene instalaciones eléctricas de equipo de cómputo independiente de otras instalaciones eléctricas?	10	7	
5	¿Se tiene reguladores para los equipos de cómputo?	10	5	
6	¿Existe tableros de distribución eléctrica?	10	4	
7	¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlo?	10	5	

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 03-12-2012
REVISADO POR: L.F.P.G	FECHA: 03-12-2012

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
FASE II REVISIÓN Y EVALUACIÓN DE CONTROLES Y SEGURIDADES
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

M/E.C 4/9

MATRIZ DE EVALUACIÓN DE CONTROL INTERNO SEGURIDADES EN INSTALACIONES				
	PREGUNTA	**Pon.**	**Calif.**	**Responsable**
8	¿Cuenta la División Redes con una fuente de poder capaz de dar energía al computador cuando se suprime la corriente eléctrica?	10	3	Técnico de las D.R
9	¿La instalación eléctrica de la División Redes tiene conexión con la tierra?	10	7	
10	¿Si existe un estudio de carga del consumo de los equipos que están instalados?	10	9	
	TOTAL	**100**	**61**	

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 03-12-2012
REVISADO POR: L.F.P.G	FECHA: 03-12-2012

DETERMINACIÓN DEL RIESGO SEGURIDADES EN INSTALACIONES

NC = CT/PT
NC = 61/ 100 = 0.61 X 100 = 61 **%**

RIESGO DE CONTROL

ALTO	MODERADO	BAJO
15.50%	51.75%	76.95%
BAJO	**MODERADO**	**ALTO**

NIVEL DE CONFIANZA

Conclusión: Como se pudo apreciar hemos obtenido una calificación de riesgo 61% que nos da un nivel de confianza moderado con un riesgo moderado, de modo que la División Redes si especifica cómo están realizadas cada una de sus instalaciones.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 03-12-2012
REVISADO POR: L.F.P.G	FECHA: 03-12-2012

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
FASE II REVISIÓN Y EVALUACIÓN DE CONTROLES Y SEGURIDADES
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

M/E.C 6/9

MATRIZ DE EVALUACIÓN DE CONTROL INTERNO SEGURIDADES EQUIPO DE CÓMPUTO				
	PREGUNTA	**Pon.**	**Calif**	**Responsable**
1	¿Se tiene inventarios actualizados de los equipos y terminales con su localización?	10	5	Técnico de las D.R
2	¿Se tiene seguros sobre todos los equipos que posee la División Redes?	10	6	
3	¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo?	10	6	
4	¿Si algún equipo ya es obsoleto, o no se está utilizando existe algún procedimiento para sustituir con un nuevo equipo?	10	6	
5	¿Existe un lugar suficiente para todos los equipos que dispone la División Redes?	10	3	
6	¿Qué topología de Red utilizan las computadoras de la División Redes?	10	5	
7	¿El gabinete que resguarda al RACK cuenta con ventiladores?	10	5	
8	¿Los cables de transmisión de datos son certificados y debidamente etiquetados?	10	4	
	TOTAL	**80**	**40**	

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 03-12-2012
REVISADO POR: L.F.P.G	FECHA: 03-12-2012

DETERMINACIÓN DEL RIESGO SEGURIDADES EQUIPO DE CÓMPUTO

NC = CT/PT
NC = 40/ 80 = 0.50 X 100 = 50 **%**

RIESGO DE CONTROL

ALTO	MODERADO	BAJO
15.50%	51.75%	76.95%
BAJO	**MODERADO**	**ALTO**

NIVEL DE CONFIANZA

Conclusión: como se puede observar una calificación de riesgo 50% que nos da un nivel de confianza bajo con un riesgo alto, esto indica que División Redes no dispone con suficiente espacio para sus equipos ya que lo comparten con la División Informáticos.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 03-12-2012
REVISADO POR: L.F.P.G	FECHA: 03-12-2012

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
FASE II REVISIÓN Y EVALUACIÓN DE CONTROLES Y SEGURIDADES
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

M/E.C 8/9

MATRIZ DE EVALUACIÓN DE CONTROL INTERNO

SEGURIDADES PARA EL PERSONAL

	PREGUNTA	Pon.	Calif.	Responsable
1	¿Existe una persona responsables de la seguridad en la División Redes?	10	9	Jefe de la D.R
2	¿Es reconocido el trabajo fuera de horarios al personal?	10	3	
3	¿Se identifica a las personas que ingresa a la División Redes?	10	8	
4	¿Existe algún indicador de que está prohibido fumar?	10	6	
5	¿Realizan capacitaciones al personal que está laborando dentro de la División Redes?	10	8	
6	¿Existen políticas de vacaciones obligatorias al personal de la División Redes?	10	6	
7	¿Existe separación de funciones y de responsabilidades en la División Redes?	10	5	
8	¿Existe política para mantener la seguridad cuanta termina la relación laboral con un empleado?	10	8	
	TOTAL	**80**	**53**	

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 03-12-2012
REVISADO POR: L.F.P.G	FECHA: 03-12-2012

DETERMINACIÓN DEL RIESGO SEGURIDADES PERSONAL

NC = CT/PT
NC = 53/ 80 = 0.66 X 100 = 66 **%**

RIESGO DE CONTROL

ALTO	MODERADO	BAJO
15.50%	51.75%	76.95%
BAJO	**MODERADO**	**ALTO**

NIVEL DE CONFIANZA

Conclusión: se puede verificar que el personal de la División Redes tiene una calificación de riesgo 66% que nos da un nivel de confianza moderado con un riesgo moderado, esto indica que División Redes dispone con un buen personal capacitado constantemente para que puedan realizar un trabajo de una mejor manera.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 03-12-2012
REVISADO POR: L.F.P.G	FECHA: 03-12-2012

1.6 INFORME SOBRE LA EVALUACIÓN DE LA ESTRUCTURA DE CONTROL INTERNO TOMANDO EN BASE AL CUMPLIMIENTO DE LA FASE

Al revisar el control interno de manera general la organización presenta deficiencias en la segregación de funciones por que cuenta con un reducido número de personal lo que afecta la atención al cliente, debido a la prestación de sus servicios a nivel nacional.

La infraestructura de la División Redes e muy reducida, además se encuentra en malas condiciones debido a la falta de mantenimiento, esto ocasiona que el personal no labore correctamente ya que tiene que respira mucho polvo que expiden las paredes.

Los equipos de cómputo no tienen un debido control de inventario el cual puede ocasionar la perdida de los mismos, además no se realiza mantenimientos a los equipos con frecuencia, únicamente revisan cuando ya está fallando y esto puede generar pérdidas económicas a la institución.

En cuanto a las instalaciones se puede apreciar que no cuentan con una fuente de poder capaz de dar energía al computador cuando se suprime la corriente eléctrica, interrumpiendo de esta manera las labores.

De tal forma que el Equipo de Auditoria concluye que la auditoría debe continuar determinando sus respectivas conclusiones y recomendaciones.

Latacunga a 07 de Diciembre del 2012

Atentamente.

……
Egda. Susana Bastidas
Consulexer S.A.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 07-12-2012
REVISADO POR: L.F.P.G	FECHA: 07-12-2012

3.6.3 Fase III Examen Detallado de Áreas Críticas

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
ÍNDICE DE LA FASE III EXAMEN DETALLADO DE ÁREAS CRÍTICAS
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

F III

	CONTENIDO	REF.
	Programa de Auditoría	P/A 4/9
1.1	Memorándum de Planificación Específica	M/P.E 1/2
1.2	Programas de Auditoría por componente	
	-Edificio	P/A 5/9
	-Instalaciones	P/A 6/9
	-Equipo de Cómputo	P/A 7/9
	-Personal	P/A 8/9
1.3	Hoja de Puntos de Control Interno	PCI 1/2
1.4	Informe de Cumplimiento fase III	I/C 3/3

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 17-12-2012
REVISADO POR: L.F.P.G	FECHA: 17-12-2012

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
PROGRAMA DE AUDITORÍA
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

P/A 4/9

OBJETIVO

- ✓ Determinar la eficiencia de los equipos e instalaciones con las que cuenta la División Redes, mediante la aplicación de procedimientos e instrumentos acorde a las necesidades del auditor.

Nº	PROCEDIMIENTO	REF. P/T	ELABORADO POR:	
			AUDITOR	FECHA
1	Elaborar un Plan Específico de Auditoría.	M/P.E 1./2	Consulexter S.A	02-01-2013
2	Elaborar Programas de Auditoría por cada componente: -Edificio -Instalaciones -Equipo de Cómputo -Personal	P/A 5/9 P/A 6/9 P/A 7/9 P/A 8/9	Consulexter S.A	04-01-2013
3	Elaborar una Hoja de Apuntes sobre los hallazgos encontrados en la Auditoría.	PCI 1/2	Consulexter S.A	24-01-2013
4	Elaborar el informe de cumplimento de la fase.	I/C 3/3	Consulexter S.A	25-01-2013

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 17-12-2012
REVISADO POR: L.F.P.G	FECHA: 17.12.2012

1.1 MEMORÁNDUM DE PLANIFICACIÓN ESPECÍFICA

Empresa Auditada: Dirección Nacional de Telecomunicaciones e Informática de la Policía Nacional "División Redes".
Tipo de Auditoria: Auditoría Informática a la Seguridad Física
Periodo: 01 de octubre del 2012 al 31 de enero del 2013
Preparado por: Consulexter S.A.
Responsables: Jefe Egda. Susana Bastidas, Supervisor Ing. Patricia López.
Fecha de Emisión: 02/01/2013

Contenido:

Objetivos de la visita final:

Verificar la seguridad de los equipos e instalaciones con la que cuenta la División Redes.

Matriz de decisiones por componente:

Luego de haber efectuado la respectiva observación de los departamentos con las que cuenta, se concluye que el riesgo inherente que existe en estos departamentos es moderado por consiguiente el riesgo de control es bajo el control clave que se ha establecido como control clave la eficiencia de la comunicación de información.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 02-01-2013
REVISADO POR: L.F.P.G	FECHA: 02-01-2013

Programas de Auditoría:

De acuerdo con el análisis realizado en los programas se persiguen objetivos específicos como: determinar la eficiencia y eficacia de los equipos e instalaciones que a diario labora, de la misma manera la utilización de la información.

Personal Requerido:

- **Tutora**: Ing. Patricia López
- **Auditor Jefe:** Egda. Susana Bastidas
- **Auditor Supervisor**: Ing. Patricia López
- **Auditor Sénior:** Egda. Ana Calero

Tiempo Estimado:

Quince días, cinco horas diarias de trabajo.

Firmas:

……..	……...
Susana Bastidas	Ing. Patricia López
Auditor Jefe	**Auditor Supervisor**

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 02-01-2013
REVISADO POR: L.F.P.G	FECHA: 02-01-2013

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
FASE III EXAMEN DETALLADO DE ÁREAS CRÍTICAS
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

P/A 5/9

PROGRAMA DE AUDITORÍA EDIFICIO				
ACTUACIÓN: Auditoría a la Seguridad Física				
ÁMBITO: División Redes de la Dirección Nacional de Telecomunicaciones e Informática				
OBJETIVO: Realizar un examen detallado de la Seguridad Física del edificio para el aprovechamiento de espacio.				
N°	**PROCEDIMIENTOS**	**REF. P/T**	**ELABORADO POR**	
			AUDITOR	**FECHA**
1	Verificar la existencia de salidas de emergencia, y de cámaras de seguridad.	S/C 1/1	B.B.S.M/C.Y.A.R	08-01-2013
2	Verificar las condiciones físicas del aire acondicionado y de las alarmas contra incendios.	A/A 1/1	B.B.S.M/C.Y.A.R	09-01-2013
3	Verificar la existencia de extintores de fuego.	E/F 1/1	B.B.S.M/C.Y.A.R	10-01-2013

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 04-01-2013
REVISADO POR: L.F.P.G	FECHA: 04-01-2013

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
FASE III EXAMEN DETALLADO DE ÁREAS CRÍTICAS
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

P/A 6/9

PROGRAMA DE AUDITORÍA INSTALACIONES				
ACTUACIÓN: Auditoría a la Seguridad Física				
ÁMBITO: División Redes de la Dirección Nacional de Telecomunicaciones e Informática				
OBJETIVO: Determinar la efectividad de la estructuración de las conexiones eléctricas de la División Redes.				
N°	**PROCEDIMIENTOS**	**REF. P/T**	**ELABORADO POR**	
			AUDITOR	**FECHA**
1	Verificar que los cables de las instalaciones se encuentren debidamente ubicados y etiquetados.	C/E 1/1	B.B.S.M/C.Y.A.R	11-01-2013
2	Verificar que exista conexión a tierra física.	T/F 1/1	B.B.S.M/C.Y.A.R	14-01-2013
3	Verificar la existencia de generadores de energía.	G/E 1/1	B.B.S.M/C.Y.A.R	15-01-2013

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 04-01-2013
REVISADO POR: L.F.P.G	FECHA: 04-01-2013

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
FASE III EXAMEN DETALLADO DE ÁREAS CRÍTICAS
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

P/A 7/9

PROGRAMA DE AUDITORÍA EQUIPO DE CÓMPUTO				
ACTUACIÓN: Auditoría a la Seguridad Física				
ÁMBITO: División Redes de la Dirección Nacional de Telecomunicaciones e Informática				
OBJETIVO: Realizar un examen				
N°	**PROCEDIMIENTOS**	**REF. P/T**	**ELABORADO POR**	
			AUDITOR	**FECHA**
1	Elaborar una cédula analítica de los inventarios de los Equipos de Cómputo que posee la División Redes.	INV 1/1	B.B.S.M/C.Y.A.R	16-01-2013
2	Obtener el diseño de la Red, evaluando la ubicación y funcionalidad de los terminales.	D/R 1/1	B.B.S.M/C.Y.A.R	17-01-2013
3	Verificar la existencia de dispositivos de respaldo de información y la existencia de un Plan de Contingencia Informático.	R/P.C 1/1	B.B.S.M/C.Y.A.R	18-01-2013

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 04-01-2013
REVISADO POR: L.F.P.G	FECHA: 04-01-2013

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
FASE III EXAMEN DETALLADO DE ÁREAS CRÍTICAS
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

P/A 8/9

PROGRAMA DE AUDITORÍA PERSONAL				
ACTUACIÓN: Auditoría a la Seguridad Física				
ÁMBITO: División Redes de la Dirección Nacional de Telecomunicaciones e Informática				
OBJETIVO: Realizar un examen				
N°	**PROCEDIMIENTOS**	**REF. P/T**	**ELABORADO POR**	
			AUDITOR	**FECHA**
1	Verificar los contratos de trabajo del personal que labora en la División Redes	C/T 1/1	B.B.S.M/C.Y.A.R	21-01-2013
2	Elaborar una cédula narrativa del cumplimiento de funciones asignadas al personal, verificando nivel académico y experiencia laboral.	C/F 1/1	B.B.S.M/C.Y.A.R	22-01-2013
3	Comprobar el uso adecuado del sistema Biométrico que posee el Departamento.	S/B 1/1	B.B.S.M/C.Y.A.R	23-01-2013

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 04-01-2013
REVISADO POR: L.F.P.G	FECHA: 04-01-2013

√ Se constató que no existe señalización alguna sobre salidas de emergencia del edificio, la cual posee una única entrada y salida del personal. (Ver H.A 1.1)

Además la División Redes cuenta con un guardia para vigilar el ingreso tanto del personal como de personas ajenas, las 24h00 del día en turnos rotativos, dicho guardia realiza los registros en un libro donde anota nombres y apellidos, lugar al que desea ingresar, nombre de la persona quien le espera y solicita su identificación, para entregar una de visitante, asimismo posen una cámara de vigilancia que funciona las 24 horas del día independientemente del grado de iluminación que haya a su alrededor. De esta forma la cámara capta imágenes a todo color, claras y nítidas mientras exista suficiente iluminación y pasa automáticamente a modo blanco y negro cuando se detecta un nivel bajo de luz. Los infrarrojos son operativos en una distancia de hasta 40 metros.

√ Cuentan con un sistema de aire acondicionado de precisión Liebert DS, 28-105kW en el centro de datos brindando un control fiable, preciso y eficiente de la temperatura, humedad y flujo de aire de la sala para un funcionamiento apropiado del equipo electrónico crítico. El sistema flexible Liebert DS ofrece una alta eficiencia energética, un control amigable con el usuario, marco modular, acceso frontal para mantenimiento y opciones de compresor y ventilador, además se puede observar que se encuentra en perfecto estado ya que recibe mantenimiento preventivo una vez al año y correctivo cuando es necesario.

√ Se observa sensores de humo, el cual posee una cámara que permite verificar la sensibilidad del detector mediante la simple observación de la frecuencia de destello del LED, la cual provee inmunidad superior a las falsas alarmas generadas por el polvo ambiental, el LED destella una luz roja para indicar un problema de calibración y permanece encendido ante una alarma que se activa automáticamente, además cuentan con alarmas que pueden ser encendidas manualmente y se encuentran en lugares accesibles.

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
EDIFICIO
Auditoría Informática a la Seguridad Física
en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

E/F 1/1

Extintores

√En toda la institución se cuenta con extintores de fuego especialmente donde se encuentra el centro de datos, el cual muestra las siguientes especificaciones: Extintor portátil de gran capacidad de extinción, cargado con Gas Carbónico (Co2), especial para incendio de líquidos inflamables, es un gas inodoro, asfixiante, congelante, auto presurizante (Los extintores de CO2 no dejan ningún tipo de residuo después de su utilización por lo que puede ser utilizado sin necesidad de limpiar luego la zona), válvula en bronce, de gran capacidad de descarga y tubo sifón en plástico de gran resistencia, manijas en lámina color negro, y provista de un pasador de gran dureza.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 10-01-2013
REVISADO POR: L.F.P.G	FECHA: 10-01-2013

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
FASE III EXAMEN DETALLADO DE ÁREAS INSTALACIONES
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

C/E 1/1

√Se realizó una constatación física sobre los cables de las instalaciones estén debidamente etiquetados, mismo que se encuentran con sus debidas etiquetas salvo el caso de los cables de transmisión de datos los cuales no se encuentran certificados y etiquetados debido a la falta del sistema certificador de cables de transmisión de datos.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 11-01-2013
REVISADO POR: L.F.P.G	FECHA: 11-01-2013

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
INSTALACIONES
Auditoría Informática a la Seguridad Física
en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

T/F 1/1

√Se realizó una constatación física sobre las conexiones a tierra física mismo que se encuentro con sus respectivas conexiones dentro de la División Redes , además se comprueba que se realizan la mediciones de resistencia de los electrodos de puesta a tierra, asimismo las conexiones se encuentran en buenas condiciones físicas y en base a nuestro estudio dicha instalación se realizan bajo las especificaciones técnicas que brinda las diferentes instituciones encargadas del adecuado manejo a través de normas y códigos como es el caso de: Normas IEC (International Electrotechnical Commission), Código Eléctrico Nacional (Ecuatoriano) NEC, Código Empresa Eléctrica

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 14-01-2013
REVISADO POR: L.F.P.G	FECHA: 14-01-2013

√ Poseen un generador de energía que se activa automáticamente las 24 horas del día de toda la semana en caso de interrupción de la energía de red pública, ya que el mismo almacena la energía en unas baterías, además para cada equipo de cómputo se cuenta con UPS, que da una duración de energía de 10 a 12 minutos para guardar la información y apagar los equipos.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 15-01-2013
REVISADO POR: L.F.P.G	FECHA: 15-01-2013

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
EQUIPO DE CÓMPUTO
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

INV. 1/5

N°	Sección	Descripción	Serie	Marca	Características	Observaciones
1	Ingeniería	Computadora	2UA202061B	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado
2	Ingeniería	Computadora	2UA2151MS7	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado
3	Ingeniería	Computadora	2UA2151BXY	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 16-01-2013
REVISADO POR: L.F.P.	FECHA: 16-01-2013

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
EQUIPO DE CÓMPUTO
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

INV. 2/5

N°	Sección	Descripción	Serie	Marca	Características	Observaciones
4	Ingeniería	Computadora	2UA202061L	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado
5	Operaciones	Computadora	2UA034004V	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado
6	Operaciones	Computadora	2UA2080V8H	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 16-01-2013
REVISADO POR: L.F.P.	FECHA: 16-01-2013

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
EQUIPO DE CÓMPUTO
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

INV. 3/5

N°	Sección	Descripción	Serie	Marca	Características	Observaciones
7	Operaciones	Computadora	MXJ94706YJ	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado
8	operaciones	Computadora	2UA1450NMT	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado
9	Administración Sistema Troncalizado	Computadora	MXJ94706S6	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 16-01-2013
REVISADO POR: L.F.P.	FECHA: 16-01-2013

N°	Sección	Descripción	Serie	Marca	Características	Observaciones
10	Administración Sistema Troncalizado	Computadora	2UA040JSP	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado
11	Administración Sistema Troncalizado	Computadora	2UA0440K15	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado
12	Administración Sistema Troncalizado	Computadora	2UA2151MVO	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 16-01-2013
REVISADO POR: L.F.P.	FECHA: 16-01-2013

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
EQUIPO DE CÓMPUTO
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

INV. 5/5

N°	Sección	Descripción	Serie	Marca	Características	Observaciones
13	Operaciones	Computadora	2UA202061V	Hewlett-Packard	Memoria RAM: 1,00GHz Procesador Intel Pentium Dual Core de 2.6GHz Sistema Operativo: Windows XP Disco Duro: 320GHz	Buen estado
14	operaciones	Impresora laser	MXJ9470832	Hewlett-Packard	Impresora B/n, color alta resolución	Buen estado
15	Administración Sistema Troncalizado	Computadora Portatil	H8758M1	DELL	Memoria RAM: 4,00GHz Procesador Intel Core i3 de 2.2GHz Sistema Operativo: Windows VISTA Disco Duro: 500 GHz	Buen estado

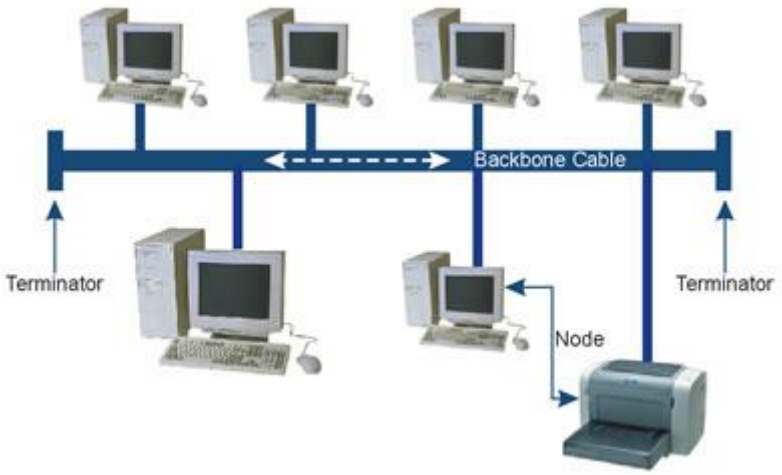
CONCLUSIÓN

√No se encontró registro alguno del inventario de Equipo de Cómputo y únicamente se realizó una constatación física de lo disponible en ese momento. (Ver H.A)

Se ha determinado los atributos y características técnicas de los equipos de cómputo convenientes para el cumplimiento de las actividades operativas en la institución.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 16-01-2013
REVISADO POR: L.F.P.	FECHA: 16-01-2013

√ Se verificó que utilizan la Red LAN, para todos los equipos existentes, tanto computadores como impresoras, utilizando además una topología en bus la cual consiste en que los nodos se unen en serie con cada nodo, conectado a un cable largo denominado backbone, formando un único segmento para lo cual los extremos del cable se terminan con una resistencia de acople denominada terminador, que además de indicar que no existen más ordenadores en el extremo, permiten cerrar el bus por medio de un acople de impedancias.



ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 17-01-2013
REVISADO POR: L.F.P.G	FECHA: 17-01-2013

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
EQUIPO DE CÓMPUTO
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

R/P.C 1 /1

RESPALDOS

√El respaldo se obtiene en digital mediante una unidad de almacenamiento, de tal forma que el sistema se encarga automáticamente de respaldarlo, todos los archivos se encuentra localizado en el centro de datos, además se realiza descargas periódicas de la información en Cd., mismo que son archivados en un lugar seguro evitando así la perdida de información.

Además se verifico la que la División Redes durante periodo auditado no posee un Plan de Contingencia para los equipos de cómputo en caso de suscitarse algún tipo de desastre, para lo cual se realizó un prototipo el cual es analizado por el jefe de la división para su puesta en marcha. (Ver H.A) y (Ver Anexo 1)

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 18-01-2013
REVISADO POR: L.F.P.G	FECHA: 18-01-2013

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
PERSONAL
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

C/T 1/1

√ La División Redes de la Dirección Nacional de Telecomunicaciones e Informática no cuenta con contratos de trabajo colectivos, debido a que se encuentran bajo la supervisión de las siguientes leyes:

Ley orgánica de servicio público

Ley orgánica de la Policía Nacional

Ley de servicios de cesantía

Ley de seguridad social de la Policía Nacional

Ley de personal

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 21-01-2013
REVISADO POR: L.F.P.G	FECHA: 21-01-2013

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
PERSONAL
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

C/F 1/1

Nomina División Redes

N°	NOMBRES	RANGO	TITULO	CARGO	EXPERIENCIA	AUDITORÍA
1	Augusto Giovanni Naranjo Rubio	Mayor.	Ing. Eléctrica y Telecomunicaciones	Jefe División Redes	6 Años	√
2	Ruth Marina Almache Moreno	Teniente.	Ing. Eléctrica y Telecomunicaciones	Jefe Secc. Ingeniería	6 Años	√
3	Fausto Javier Llerena Pazmiño	Sargento Primero.	Ing. Eléctrica y Telecomunicaciones	Técnico	5 Años	√
4	Nelly Angélica Quilligana Chamba	Cabo Segundo.	Ing. Eléctrica y Telecomunicaciones	Técnico	4 Años	√
5	Nino Moisés Simbaña Real	Cabo Segundo	Ing. Electromecánica	Técnico	4 Años	√
6	Eduardo Favio Piedra Ramírez	Mayor.	Ing. Redes de Datos	Jefe Secc. Administración	6 Años	√
7	José Miguel Gutiérrez González	Cabo Primero	Ing. Eléctrica y Telecomunicaciones	Administrador del Sistema Troncalizado	5 Años	√
8	Franklin Wilmer Pachacamac Vargas	Cabo Primero	Ing. Eléctrica y Telecomunicaciones	Administrador del Sistema Troncalizado	5 Años	√
9	Danilo Fernando Anchatipán Navas	Cabo Segundo	Ing. Informática y Sistemas Computacionales	Administrador del Sistema Troncalizado	4 Años	√
10	Víctor Hugo Sisa Amaguaya	Cabo Segundo	Ing. Eléctrica y Telecomunicaciones	Administrador del Sistema Troncalizado	4 Años	√
11	Eduardo Favio Piedra Ramírez	Mayor.	Ing. Eléctrica y Telecomunicaciones	Jefe Operaciones	6 Años	√
12	Juan Pablo Ilbay Chingo	Cabo Segundo	Ing. Eléctrica y Telecomunicaciones	Técnico	4 Años	√
13	Jaime Kléver Loachamin Quinga	Cabo Primero	Ing. Eléctrica y Telecomunicaciones	Técnico	5 Años	√
14	Víctor Armando Catota Ocapana	Cabo Segundo	Ing. Eléctrica y Telecomunicaciones	Técnico	4 Años	√

√ Además se observó que no se da cumplimiento a cada una de las funciones específicas de acuerdo a su cargo, como fue el caso de los administradores que realizan funciones adicionales de técnicos. (Ver H.A)

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 22-01-2013
REVISADO POR: L.F.P.G	FECHA: 22-01-2013

√La División Redes utiliza un reloj biométrico de huella dactilar, que controla la asistencia y a la vez el acceso a áreas restringidas, este sistema otorga gran confiabilidad y estabilidad ya que emite reportes de empleados, como es la asistencia, retrasos, salidas temprano, registra los días festivos, permisos, citas, medicas, vacaciones, comisiones, etc., además permite la asignación de horarios ya sean estos en turnos fijos o rotativos.

Asimismo posee una función de monitoreo en tiempo real para los procesos de seguridad, en donde se controla el acceso a áreas restringidas, para lo cual el personal a más de la huella dactilar debe digitalizar una clave que únicamente el personal autorizado conoce.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 23-01-2013
REVISADO POR: L.F.P.G	FECHA: 23-01-2013

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
HOJA DE APUNTES DE CONTROL INTERNO
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

PCI 1/2

HOJA DE PUNTOS DE CONTROL INTERNO

CCI

REF: P/T	CONDICIÓN	CRITERIO	CAUSA	EFECTO	CONCLUSIÓN	RECOMENDACIÓN
S/C 1/1	Falta de señalización para salidas de emergencias	La Existencia y señalización de salidas de emergencia es un requisito de funcionamiento por tanto se debe dar cumplimiento a dicha disposición.	Descuido de la administración	Aglomeración en las salidas provocando accidentes mayores en caso de algún desastre	En caso de algún siniestro no se conoce las salidas de emergencia llevando con sigo accidentes mayores	Colocar letreros indicando las diferentes salidas de emergencia.
INV 1/1	No registro de inventarios de equipo de cómputo.	Toda institución debe contar con un registro de los bienes materiales que posee el departamento para evitar robos, perdidas, etc.	Descuido del encargado de Activos Fijos.	Robos, pérdida o deterioro de los Equipos	Al no registrar estos Equipos, puede surgir la perdida y deterioro del mismo.	Elaborar el registro inmediato de los inventarios que posee la División Redes.
R/P.C 1/1	Durante el periodo auditado no contaban con un Plan de Contingencia Informático.	Toda institución debe contar con un plan de Contingencia para salvaguardar la integridad de los recursos materiales y del talento humano.	Falta de organización del personal encargado.	Perdida de información valiosa.	La División Redes no cuanta con un Plan de Contingencia que ayude a tomar medidas de prevención en caso de desastres.	Se recomienda la pronta elaboración y puesta en marcha de un Plan de Contingencia, ya que ninguna empresa o institución está exenta de algún tipo de amenaza.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 24-01.-2013
REVISADO POR: L.F.P.G	FECHA: 24-01.-2013

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
HOJA DE APUNTES DE CONTROL INTERNO
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

PCI 2/2

HOJA DE PUNTOS DE CONTROL INTERNO

CCI

REF: P/T	CONDICIÓN	CRITERIO	CAUSA	EFECTO	CONCLUSIÓN	RECOMENDACIÓN
C/F 1/1	Descripción o leyenda del Organigrama	Las instituciones deben dar a conocer a sus trabajadores cual es el rol que van a desempeñar en sus lugares de trabajo para evitar cualquier inconveniente.	Desconocimiento de funciones	Conflictos entre compañeros de trabajo	El desconocimiento de las funciones específicas trae rivalidades entre compañeros debido a que cuando algo sale mal nadie se quiere hacer cargo de lo sucedido.	Establecer leyenda del organigrama que ayude a desempeñar las funciones equitativamente y de acuerdo al cargo que ocupa..

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 24-01.-2013
REVISADO POR: L.F.P.G	FECHA: 24-01.-2013

INFORME DE CUMPLIMIENTO FASE III

Como primer paso para el cumplimiento de esta fase, es elaborar un plan específico de auditoría, dicho plan sirve de guía en el cumplimiento de actividades evitando así la duplicidad de tareas, y al final obtener una valoración general del estado de la División Redes.

Empleando la técnica de observación directa se pudo observar que el edificio físicamente se encuentra en mal estado ya que despide polvo, la pintura se encuentra deteriorada no se observa señalización alguna, pero si cuenta con extintores de humo, aire acondicionado y un personal de seguridad que controla el acceso a las personas ajenas a la institución.

Mediante la aplicación de técnicas de observación fue posible determinar la operatividad de los equipos de cómputo, contado así con un buen estado físico y funcionalidad, de igual manera los cables de red, conexiones, acometidas eléctricas se encuentran debidamente etiquetados, además se realizó una constatación física en donde se pudo apreciar que no llevan un control físico de los Equipos.

En la visita realizada a la División Redes y aplicando técnicas como la observación y el rastreo, se logró establecer que no existen puestos fantasmas, debido a que en cada departamento existe el personal necesario y acorde a la necesidad, concordando así con el nivel académico de cada uno.

Aplicando la técnica de observación documental, en los contratos de trabajo, fue posible determinar que como son miembros policiales están sujetos a la Ley y Reglamento de la Policía Nacional, teniendo así todos los beneficios como son: vacaciones, alimentación, seguro, etc., cumpliendo así con la Ley Orgánica de Servicios Públicos.

Atentamente.

……
Egda. Susana Bastidas
Consulexer S.A.

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 25-01-2013
RESIDADO POR: L.F.P.G	FECHA: 25-01-2013

3.6.4. Comunicación de Resultados

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
ÍNDICE DE LA FASE IV COMUNICACIÓN DE RESULTADOS
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

F IV

	CONTENIDO	REF.
	Programa de Auditoría	P/A 9/9
1.1	CONVOCATORIA A CONFERENCIA PARA LA LECTURA DEL INFORME FINAL DE AUDITORÍA	CLIF 1/1
1.2	CARTA DE INTRODUCCIÓN DEL INFORME FINAL	CPI 1/1
1.3	INFORME FINAL DE AUDITORÍA	IF 1/6
1.4	PLAN DE MEJORA	PM 1/1

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 28-01-2013
REVISADO POR: L.F.P.G	FECHA: 28-01-2013

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
PROGRAMA DE AUDITORÍA
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

P/A 9/9

OBJETIVO

- ✓ Comunicar a las autoridades de la División Redes de la Dirección Nacional de Telecomunicaciones e Informática, los hallazgos encontrados en el proceso de Auditoría.

Nº	PROCEDIMIENTO	REF. P/T	ELABORADO POR:	
			AUDITOR	FECHA
1	Preparar y entregar las convocatorias a conferencia para la lectura del Informe Final de Auditoría.	CLIF 1/1	Consulexter S.A	29-01-2013
2	Diseñar y elaborar la carta de presentación del Informe de Auditoría.	CPI 1/1	Consulexter S.A	29-01-2013
3	Elaborar el Informe Final de Auditoría.	IF 1/6	Consulexter S.A	29-01-2013
4	Elaboración del Plan de Mejora con respecto a la Auditoría.	PM 1/1	Consulexter S.A	08-02-2013

ELABORADO POR: B.B.S.M./C.Y.A.R.	FECHA: 28-01-2013
REVISADO POR: L.F.P.G	FECHA: 28-01-2013

1.1 CONVOCATORIA A CONFERENCIA PARA LA LECTURA DEL INFORME FINAL DE AUDITORÍA.

Latacunga, 29 de Enero del 2013

Crnl. Jaime Bladimir Jara López
DIRECTOR NACIONAL DE TELECOMUNICACIONES E INFORMÁTICA
Presente.

De mi consideración:

De conformidad con lo dispuesto en los artículos 90 de la Ley Orgánica de la Contraloría General del Estado y 23 de su Reglamento, convoco a usted a la conferencia final de comunicación de resultados mediante la lectura del borrador del informe de Auditoría Informática a la Seguridad Física, en la División Redes de la Dirección Nacional de Telecomunicaciones e Informática de la Policía Nacional, por el período comprendido entre el 1 de octubre del 2012 al 31 de enero del 2013, realizado en cumplimiento del trabajo investigativo previo a la obtención del Título de Ingeniería en Contabilidad y Auditoría.

La diligencia se llevará a cabo en las instalaciones de la Dirección Nacional de Telecomunicaciones e Informática de la Policía Nacional, ubicada en el sector La Gasca en las calles Ritter Oe 9-141 y Diego Zorrilla (Quito), el día 8 de Febrero del 2013 a las 9:30 a.m. En caso de no poder asistir personalmente, agradeceré notificar por escrito, indicando los nombres, apellidos y número de cédula de ciudadanía de la persona que participará en su representación.

Atentamente,

…….
Egda. Susana Bastidas
JEFE DE EQUIPO DE AUDITORÍA

CONSULEXTER S.A.
AUDITORES INDEPENDIENTES
CARTA DE PRESENTACIÓN DEL INFORME FINAL
Auditoría Informática a la Seguridad Física en la División Redes de la D.N.T.I.P.N
Del 1 de octubre del 2012 al 31 de enero del 2013

CPI 1/1

Señores;
Dirección Nacional de Telecomunicaciones e Informática
Presente:

Hemos realizado una Auditoría Informática a la Seguridad física de la Dirección Nacional de Telecomunicaciones e Informática con el objetivo de evaluar lo siguiente:

Eficiencia y eficacia del uso de los sistemas informáticos, para verificar la utilización y el manejo de los mismos, y el cumplimiento de políticas de seguridades físicas implantadas.

Nuestro examen se realizó de acuerdo con las normas para el ejercicio Profesional de la Auditoría Informática promulgadas por el instituto de auditores, en consecuencia se aplicó las Técnicas y Procedimientos de Auditoría que consideramos necesarios.

Para la evaluación de los sistemas utilizamos parámetros propios de la empresa y aquellos que se aplican dentro de una administración eficiente y honesta.

Nuestro informe contiene comentarios, conclusiones y recomendaciones para mejoras reales y potenciales.

Las recomendaciones han sido discutidas y aceptadas por el jefe de área del centro de cómputo con quien hemos desarrollado un plan de mejoras para monitorear la implementación.

A la vez dejamos constancia de nuestro reconocimiento por tal colaboración que hemos recibido en nuestro trabajo.

Atentamente:

…….
Egda. Susana Bastidas
Consulexer S.A.

INFORME DE AUDITORÍA INFORMÁTICA A LA SEGURIDAD FÍSICA EN LA DIVISIÓN REDES DE LA DIRECCIÓN NACIONAL DE TELECOMUNICACIONES E INFORMÁTICA

a.- Fecha de Inicio: 08 de Febrero del 2013.

b.- Nombre de los Auditores:

Egda. Susana Bastidas

JEFE DE EQUIPO

Ing. Patricia López

SUPERVISOR

Egda. Ana Calero

AUDITOR SÉNIOR

c.- Lista de las personas entrevistadas:

Crnl. Jaime Jara	Director Nacional de Telecomunicaciones e Informática.
Mayr. Giovanni Naranjo Rubio	Jefe de la División Redes

MOTIVO DE LA AUDITORÍA

La Auditoría a la Seguridad Física a la División Redes se llevó a efecto ante la necesidad de evaluar la seguridad física de los equipos, instalaciones, infraestructura y al personal, ya que no se ha realizado antes este tipo de trabajos, además será de gran utilidad como base para futuras investigaciones.

OBJETIVO DEL EXAMEN:

Revisar y verificar el centro de datos, para determinar si cumple o no con aspectos necesarios de seguridad física analizando los manuales, políticas o planes de seguridad comprendido por el ejercicio del 1 de octubre del 2012 al 31 de enero del 2013, a fin de emitir un informe donde se exprese conclusiones y recomendaciones de todos los hallazgos encontrados, para que la dirección pueda tomar medidas correctivas de manera adecuada.

Objetivos específicos:

- ✓ Determinar los componentes que se van analizar para desarrollar un control interno adecuado
- ✓ Describir los hallazgos que perjudique la seguridad de los equipos de cómputo y del personal en base a las normativas establecidas.
- ✓ Dar a conocer las conclusiones y recomendaciones a la alta dirección de la institución, por medio de un informe.

ALCANCE DE LA AUDITORÍA

Esta Auditoría Informática a la Seguridad Física cubrió el periodo del 1 de octubre del 2012 al 31 de enero del 2013 en los cuales se examinó la Seguridad Física de los equipos e instalaciones, documentación, cumplimiento de políticas establecidas en relación a la seguridad.

PROCEDIMIENTOS APLICADOS

En los procedimientos aplicados se puede mencionar que realizamos una evaluación para medir la seguridad física del centro de datos y del personal de la División Redes, en donde hicimos referencia a los siguientes componentes:

- ✓ Edificio
- ✓ Instalaciones
- ✓ Equipo de cómputo y;
- ✓ Personal

El cual cada uno de ellos fue analizado tomando en cuenta un cuestionario de Control Interno, en donde permitió determinar el nivel de confianza y de riesgo con el que cuenta dichos componentes.

Una vez realizada la identificación de cada uno de los componentes; se determinaron los siguientes hallazgos:

EDIFICIO

HALLAZGO 1.- FALTA DE SEÑALIZACIÓN PARA SALIDAS DE EMERGENCIAS

CRITERIO 1

La existencia y señalización de salidas de emergencia es un requisito de funcionamiento para las instituciones sean estas públicas o privadas, por tanto se debe dar cumplimento a dicha disposición.

CONCLUSIÓN 1

Se verifico que no existe señalización de salidas de emergencia en toda la institución especialmente en el área del centro de datos, además las paredes se encuentran en mal estado físico debido al tiempo que lleva sin mantenimiento, ocasionando malestar en el personal que trabaja en el área debido al polvo que despide de las paredes.

RECOMENDACIÓN 1

Se recomienda realizar un mantenimiento general del edificio adecuado especialmente el centro de datos y abriendo otras alternativas de salidas con sus respectivos letreros de aviso.

EQUIPO DE CÓMPUTO

HALLAZGO 2.- NO EXISTE REGISTRO DE INVENTARIOS DE EQUIPO DE CÓMPUTO

CRITERIO 2

Toda institución debe contar con un registro de los bienes materiales que posee el departamento para evitar robos, pérdidas o deterioro de Equipos.

CONCLUSIÓN 2

No se tiene un control de las características y estado de los equipos que se encuentran instalados en cada departamento de la institución.

RECOMENDACIÓN 2

Se recomienda tener un inventario detallado de los equipos donde se incluyan hardware: dispositivos instalados en cada máquina, números de series, ubicación de los equipos y demás datos sobre procesadores, tarjetas, teclados, computadoras personales y programas informáticos, basándose en lo Principios de Contabilidad Generalmente Aceptados. (Bienes Económicos).

HALLAZGO 3.- CARENCIA DE UN PLAN DE CONTINGENCIA

CRITERIO 3

Según la Norma de Control Interno 410 titulada Tecnología de la Información, referente a 410-11 Plan de Contingencias:

Corresponde a la máxima autoridad la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.

CONCLUSIÓN 3

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

RECOMENDACIÓN 3

Declarar la elaboración, aprobación e implementación de un Plan de Continuidad considerada necesaria para minimizar las consecuencias de la interrupción del servicio. Además este plan establecerá, organizará y documentará los riesgos, responsabilidades, políticas, procedimientos y acuerdos, así mismo, proporcionará un enfoque organizado y consolidado para dirigir actividades de respuesta y recuperación ante cualquier incidente o interrupción de operaciones imprevista, evitando confusión y reduciendo la situación de tensión.

PERSONAL

HALLAZGO 4.- DESCRIPCIÓN O LEYENDA DEL ORGANIGRAMA

CRITERIO 4

Al no haber responsabilidades puntuales asignadas duplicación lo que genera una pérdida de productividad.

CONCLUSIÓN 4

Se evidencio durante la revisión realizada en la División Redes que no se tiene una segregación de funciones adecuada, debido a que cuentan con poco personal especializado en el área de las TIC´S.

RECOMENDACIÓN 4

Se recomienda tener una definición clara de funciones para los diferentes cargos que se tienen en la División Redes, además adquirir más elementos policiales especializados en el área informática para así poder cumplir con la demanda de atención a las diferentes unidades policiales.

Para constancia firman:

…… ……..

Egda. Susana Bastidas — **JEFE DE AUDITORÍA**

Mayr. Geovanny Naranjo — **JEFE DE LA DIVISION REDES**

3.7 Plan de Mejora

Recomendación	Tarea	Responsable	Tiempos Inicio-fin	Recursos necesarios	Financiamiento	Indicador de seguimiento	Responsable seguimiento
Colocar letreros de salidas de emergencia	Colocación de letreros	Técnico de Mantenimiento	Abril - Diciembre 2013	Letreros	El presupuesto de gastos varios	Observación directa	Consulexter S.A
Difusión del Plan de Contingencia	Difundir las normas y políticas de seguridad informática.		Marzo –Abril del 2013	Copias e infocus	Ninguno	Plan de Contingencia	Consulexter S.A
Registro de inventarios	Realizar una toma física de los equipos que posee.	Encargado de Activos Fijos	Marzo – Abril 2013	Computadora	Ninguno	El registro de inventarios	Consulexter S.A
Establecer leyenda del organigrama	Elaborar un manual de funciones.	Jefe de Recursos Humanos	Marzo – Abril 2013	Computadora y hojas	Ninguno.	Manual de funciones	Consulexter S.A

…… ……. ……..

Egda. Susana Bastidas — **JEFE DE AUDITORÍA**

Crnl. Jaime Jara — **DIRECTOR NACIONAL D.NT.I.P.N.**

Mayr. Geovanny Naranjo — **JEFE DE LA DIVISIÓN REDES**

3.8. Conclusiones

La División Redes no cuenta con una Auditoría Informática a la Seguridad Física por lo cual se aplicó la misma dando los siguientes resultados:

- ✓ Existe poca bibliografía referente a este tema, pero se realiza la revisión de la información de las fuentes bibliográficas electrónicas e impresas existentes, logrando desarrollar las categorías fundamentales del marco teórico que sustentaron el desarrollo de la investigación, en base a criterios de autores que escriben sobre este tema.

- ✓ Al aplicar las técnicas de investigación se pudo observar que no existe salidas de emergencia ni señalización alguna, provocando la aglomeración de los empleados en casos de alguna emergencia.

- ✓ La Aplicación de una Auditoria la Seguridad Física permite garantizar la seguridad física de los equipos de cómputo, instalaciones, edificio y del personal, el mismo que fortalecerá el buen desarrollo de la División Redes.

- ✓ No cuenta con un Plan de Contingencia, mismo que representa gran importancia para el desarrollo de la institución.

- ✓ No se encontró la documentación pertinente de los inventarios de los Equipos de Cómputo y únicamente se realizó la constatación física por parte de las investigadoras.

3.9. Recomendaciones

- ✓ Se recomienda que la biblioteca de la Universidad Técnica de Cotopaxi, cuente con más bibliografía impresa referente a Auditoría de Seguridades para que los estudiantes tengan una base teórica y práctica.

- ✓ Se recomienda a la institución la elaboración de Auditorias a la Seguridad Física de forma periódica al igual que las demás Auditorías, ya que de estas evaluaciones depende del control, mejoramiento y prevención de riesgos en las instituciones.

- ✓ Se recomienda a la institución poner en marcha todas las recomendaciones emitidas en el informe de auditoría para el buen desempeño del centro de

- ✓ Al contar con el personal capacitado en tecnología se recomienda que la institución aproveche el talento humano para que sigan innovando en el desarrollo de nuevos programas de seguridad informática.

3.10. Referencias Bibliográficas

Bibliografía Citada

- ✓ ANDRADE, Ramiro; *Manual de la Auditoría de Gestión*; Ecuador; (2001), (Pág. 72,73).
- ✓ CASTRO, Julián, *Manual de Auditoria Informática*; (2003) (Pág. 17).
- ✓ CHIAVENATO, Idalverto, Administración de Recursos Humanos, Octava Edición, México, 2007, 31 p.
- ✓ ECHENIQUE, José A.; *Auditoría en Informática*; Ed. 2 (México, 2002), (pág. 219).
- ✓ ESTUPIÑAN, Rodrigo: *Control Interno y Fraudes*; Ed. 2, Bogotá Colombia, 2006), (pág. 25).
- ✓ FAINSTEIN, Héctor y ABADI Mauricio (2009)" Gestión Financiera, tercera edición, Ecoe Editorial, México, Pág. 45
- ✓ MADARIAGA, Juan; *Manual Práctico de Auditoría*; Ed. Deusto; (España, 2004), (pág. 13).
- ✓ MANTILLA, Samuel, Alberto, (2005) "Control Interno Informe Coso", Cuarta Edición, Ecoe Editorial, Colombia, Pág. 6-95-135-136-138.
- ✓ MARTIN, Fernando. Diccionario de Contabilidad y Finanzas. Madrid-España, Editorial ABACO Cía. Ltda., 2002. ISBN 9788480552547.
- ✓ MENDIVI E, Víctor; *Elementos de la Auditoría*; 5 Ed.; México, ECAFSA Thomson Learning, 2002. ISBN 9789706861726
- ✓ PIATTINI, Mario y DEL PESO, Emilio; *Auditoria Informática: Un Enfoque Practico*; 2 Ed.; Colombia, ALFAOMEGA, 2001. ISBN 9789701507315.

- ✓ REYES PONCE, Agustín. *Administración de empresas, teoría y práctica***.** Primera y segunda parte. México, 2004, Editorial Limusa-Wiley, SA, Pág.2. ISBN 968-18-0059-1.

- ✓ RIVAS, Gonzalo. *Auditoría Informática*; Madrid Editorial Díaz de Santos S.A, 1988. ISBN 84-87189-13-X.

Bibliografía Virtual

- ✓ *http://html.rincondelvago.com/empresa_15.html/ 10:30/08-10-2012*

- ✓ *http://html.rincondelvago.com/empresa_12.html 10:35/08-10-2012*

- ✓ *http://fccea.unicauca.edu.co/old/tgarf/tgarfse3.html/8:30/10-10-2012.*

- ✓ *http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica/11:20/10-10-2012.*

- ✓ *http://es.scribd.com/doc/18266497/METODOLOGIA-DE-LA-AUDITORIA/12:10/10-10-2012.*

3.11. Anexos