

UNIVERSIDAD TÉCNICA DE COTOPAXI

**TESIS DE GRADO PREVIO A LA OBTENCION DEL
TITULO DE INGENIERO EN INFORMATICA Y SISTEMAS
COMPUTACIONALES**

**CARRERA DE CIENCIAS DE LA INGENIERIA Y
APLICADAS**

TEMA:

**“AUDITORÍA INFORMÁTICA EN LA
COOPERATIVA DE AHORRO Y
CREDITO**

OSCUS Ltda. SUCURSAL LATACUNGA”

POSTULANTE:

MONGE HERRERA SILVANA

DIRECTOR:

Ing. EMMA CAMPAÑA RIOFRÍO

2005

LATACUNGA – ECUADOR



ENTIDAD AUTORIZADA POR LA SUPERINTENDENCIA DE BANCOS
MEDIANTE RESOLUCION N° 85-01 • DC DE 85-11-21
ALIZAR INTERMEDIACION FINANCIERA CON EL PUBLICO EN GENERAL

A petición de la parte interesada y en mi calidad de Gerente de la Cooperativa de Ahorro y Crédito "OSCUS" LTDA Sucursal Latacunga.

CERTIFICO

Que la señora: MONGE HERRERA SILVANA DEL PILAR, portadora de la cédula de ciudadanía N. 050240321-5, desarrollo una Auditoría Informática en la Cooperativa de Ahorro y Crédito "OSCUS" Ltda. Sucursal Latacunga, desde el 16 de junio de 2004 hasta el 17 de junio de 2005, demostrando capacidad, honradez, eficiencia y responsabilidad en todos sus actos y tareas encomendadas.

Es todo cuanto puedo informar en honor a la verdad, facultando al interesado hacer uso del presente documento, cuando lo estime necesario.

Latacunga, 02 de diciembre de 2005


Ing. Marco Hidalgo Guayaquil.
GERENTE SUCURSAL LATACUNGA



• **MATRIZ AMBATO:** Lalama 06-39 y Sucre • Telfs.: 282-1131 / 242-3804 / 282-2719
Fax: 282-9460 / Apartado 513
• **LATACUNGA:** Quito y Maldonado • Telfs.: 280-0008
• **PILLARO:** Av. Rumiñahui N° 10-10 • Telf.: 287-3176

• **PELILEO:** Gral. Cacha 262 y Padre Chacón • Telf.: 287-1195
• **BAÑOS:** Oriente y Alfiantes • Telf.: 274-0236
• **PATATE:** Soria y Calderón • Telf.: 287-0202

UNIVERSIDAD TÉCNICA DE COTOPAXI

CARRERA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

LATACUNGA - ECUADOR

Latacunga junio 21, 2004
CIYA-DA-372-UTC-2004

Señorita
Silvana Monge
EGRESADA CIYA – UTC
Presente

De mi consideración:

Por medio del presente pongo en su conocimiento que los señores miembros del Honorable Consejo Académico, reunidos el día 17 de junio del 2004, resolvieron: aprobar el Plan de Tesis con el tema: “AUDITORÍA INFORMÁTICA EN LA COOPERATIVA DE AHORRO Y CRÉDITO OSCUS Ltda. SUCURSAL LATACUNGA”; de su autoría, por lo que se encuentra habilitada para el desarrollo de la Tesis.

Particular que se comunica para los fines pertinentes.

Atentamente,

“POR LA VINCULACION DE LA UNIVERSIDAD CON EL PUEBLO”



Ing. Guido Yauli Chicaiza, M. Sc.
Director de la Carrera de Ciencias de la
Ingeniería y Aplicadas, Encargado



Latacunga, 11 de febrero del 2003.

Sr. Ing. Edgar Pazniño Guerrero.
GERENTE GENERAL DE LA COOPERATIVA DE AHORRO Y CRÉDITO
"OSCUS" Ltda..

Presente.-

De mi consideración.

Yo, Silvana del Pilar Monge Herrera alumna de la Universidad Técnica de Cotopaxi ubicada en la ciudad de Latacunga hago llegar a usted un cordial y atento saludo a la vez me dirijo a usted con el afán de solicitarle muy comedidamente se me permita desarrollar mi tesis en la Cooperativa de Ahorro y Crédito "OSCUS" Ltda. sucursal Latacunga, con el tema: "Auditoria Informática en la Cooperativa de Ahorro y Crédito "OSCUS" Ltda. sucursal Latacunga" dicha investigación y los resultados que arroje servirán únicamente como requisitos para obtener mi título como Ingeniero en Sistemas Computacionales sin afectar a la institución auditada, debo aclarar que mi objetivo es obtener datos reales y consistentes de usted queda acoger o no las sugerencias que se den en el informe final de la auditoria en caso que se digne en autorizar la investigación ya mencionada.

De ser positiva su respuesta solicito muy comedidamente se me haga llegar por escrito la autorización correspondiente además los límites, sectores, o aspectos a los cuales no tengo acceso para auditar.

Segura de contar con la atención favorable que se de a la presente anticipo mis debidos agradecimientos y mi compromiso de no defraudar al apoyo, apertura y confianza que se deposite en mi.

*Autorizado -
Ger. of CP Latacunga
dar las facilidades y
entregar un ejemplar de la Tesis*

AUTORIZADO
COOPERATIVA DE AHORRO
Y CRÉDITO OSCUS
GERENTE GENERAL

Atentamente


050240321-5
Egda. Silvana Monge
SOLICITANTE



GERENCIA GENERAL
FEB 13 '03 9:14

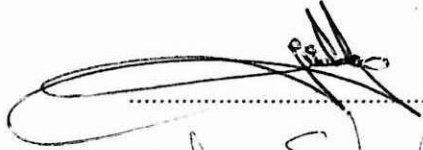
*Recibido
2032217*

CERTIFICADO

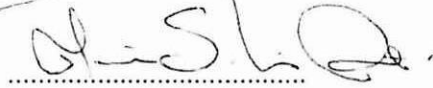
Mediante el presente certifico que la Sra. Silvana del Pilar Monge Herrera, alumna egresada de la Universidad Técnica de Cotopaxi , carrera Ciencias de la Ingeniería y Aplicadas, especialidad Ingeniería en Informática y Sistemas Computacionales, ha revisado el hardware, software, su estado físico, funcionamiento, operatividad y eficiencia, del computador a mi cargo.

Es todo cuanto puedo certificar en honor a la verdad, el portador de este documento hará uso de él, para los fines que creyere convenientes.

Ing. Marco Hidalgo **GERENCIA**



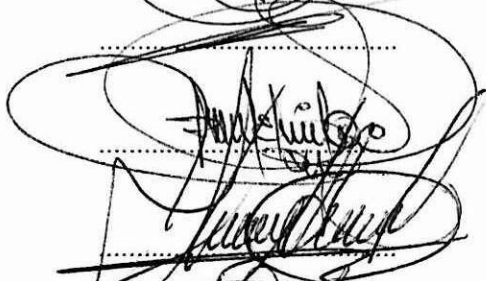
Srta. Mariana Silva **SECRETARIA**



Sra. Carmita Moya **CONTABILIDAD**



Sr. Luis Chimbo **CRÉDITO**



Sr. Raúl Gallegos **CRÉDITO**

Sr. Jonny Herrera **CAJA 1**

Sra. Sandra Rubio **CAJA 2**





ADONICIAO AUTORIZADA POR LA SUPERINTENDENCIA DE BANCOS
MEDIANTE RESOLUCION N° 85-01 - DC DE 85-11-21
PARA LA INTERMEDIACION FINANCIERA CON EL PUBLICO EN GENERAL

Ambato, 11 de Abril del 2005

CERTIFICADO

Señores Universidad Técnica de Cotopaxi

Por medio de la presente, certifico que he escuchado, discutido y corregido los resultados apuntados en el Informe Final de Auditoría Informática, efectuada en la Cooperativa de Ahorro y Crédito OSCUS Ltda. Matriz y Sucursal Latacunga, por la Sra. Silvana Monge Herrera alumna de su institución. Además manifiesto el común acuerdo de las dos partes auditor y auditado en la redacción del Informe Final, luego de las correcciones pertinentes.

Es todo cuanto puedo decir en honor a la verdad, por tanto la Sra. Silvana Monge Herrera puede hacer uso del presente certificado como a bien tenga.

Atentamente,

Ing. Carlos Santamaría.
JEFE DE SISTEMAS

AVAL

Yo, Ing. Emma Campaña Riofrío, docente de la Universidad Técnica de Cotopaxi,

CERTIFICO

Que en calidad de Director de Tesis, CERTIFICO, haber revisado minuciosamente la TESIS DE GRADO denominada: “Auditoría Informática en la Cooperativa de Ahorro y Crédito OSCUS Ltda. Sucursal Latacunga” cuya autoría pertenece a la Sra. egresada Silvana del Pilar Monge Herrera.

En tal actividad, sugiero que continúe con el trámite para la defensa de la misma

Atentamente.

Latacunga, 7 de diciembre del 2005



Ing. Emma Campaña
DIRECTOR DE TESIS
C.I.: 050220978-6

**DEL CONTENIDO DE LA PRESENTE INVESTIGACIÓN ES
RESPONSABLE EL AUTOR DE LA MISMA**

De todos los conceptos, opiniones, argumentos, conclusiones y recomendaciones, que contiene este trabajo investigativo titulado: “Auditoria Informática en la Cooperativa de Ahorro y Crédito OSCUS Ltda. Sucursal Latacunga” es responsable la autora: Sra. egresada de la especialidad de Ciencias de la Ingeniería y Aplicadas, Silvana Monge Herrera.

SILVANA DEL PILAR MONGE HERRERA

A handwritten signature in black ink, appearing to read 'Silvana Monge Herrera', with a long horizontal line extending to the right.

0502403215

UNIVERSIDAD TÉCNICA DE COTOPAXI

Informe Final

Latacunga, 7 de diciembre del 2005

Cumpliendo con lo estipulado en el capítulo IV, artículo 9 literal f del Reglamento del Curso Profesional de la Universidad Técnica de Cotopaxi, informa que la Sra. Egresada Silvana Monge, ha desarrollado su trabajo investigativo previo a la obtención de su título profesional, con la denominación: **“AUDITORÍA INFORMÁTICA EN LA COOPERATIVA DE AHORRO Y CRÉDITO OSCUS LTDA. SUCURSAL LATACUNGA”**, mismo que está acorde a los planteamientos formulados en la denuncia y construcción teórica del objeto de estudio.

El trabajo teórico cumple con el objetivo de dotar de bases conceptuales sobre la cooperativismo y Auditoría Informática.

El trabajo de investigación aporta datos estadísticos importantes que le permiten realizar un análisis de incidencia del uso de los recursos informáticos en la Cooperativa OSCUS Sucursal Latacunga, además del análisis y del trabajo investigativo se presenta un informe final de auditoría en el que se plasman todos los hallazgos, con sus respectivas conclusiones y sugerencias.

En virtud de lo antes expuesto, considero que la postulante, se encuentra habilitada para presentarse al acto de defensa de tesis.

POR LA VINCULACION DE LA UNIVERSIDAD CON EL PUEBLO,



.....
Ing. Emma Campaña Riofrío.
DIRECTOR DE TESIS
PROFESOR DE UTC.

C.C. Grupo de Tesis

AGRADECIMIENTO

Al alcanzar la meta trazada en una de las etapas de mi vida agradezco a Dios, por haber guiado con su magnificencia cada uno de mis pasos.

La gratitud es una virtud del hombre, que sabe valorar las acciones que en su beneficio se efectuaron, es así que presento mi especial agradecimiento a los Señores Cooperativa OSCUS Ltda. Sucursal Latacunga, por permitirme realizar el trabajo de Tesis de Grado, en su prestigiosa institución, por su colaboración desinteresada, por la apertura, ambiente cordial y amigable que me brindaron en todo el transcurso de la investigación.

En forma especial agradezco a la Universidad Técnica de Cotopaxi, por lo tanto a los señores catedráticos que realizan con tal esmero y cuidado sus labores docentes, de manera particular a la Ing. Emma Campaña Riofrío, quien con su don de maestro intachable, tolerante e impecable supo guiarme en forma eficaz, didáctica y pedagógica para concluir satisfactoriamente con el presente trabajo.

Y a todas las personas e instituciones que en forma directa o indirecta contribuyeron al cumplimiento del presente trabajo, ellas fueron de esencial ayuda para esclarecer interrogantes, obtener evidencias, y recopilar bases sólidas que sustenten las conclusiones, y permitan emitir sugerencias acertadas en pos del mejoramiento de la institución auditada.

GRACIAS.

DEDICATORIA

Con la satisfacción de haber alcanzado uno de mis mayores anhelos como es el de obtener un título profesional; en el que se plasmen todos y cada uno de mis esfuerzos, sacrificios y privaciones, este triunfo lo dedico a mis padres Galo Monge, Aída Herrera, y hermana Lorena, quienes con su amor inefable, con sus palabras de aliento, me apoyaron de forma incondicional en todos los aspectos, a lo largo de mi carrera universitaria.

La realización del presente trabajo se la dedico con todo cariño a mi querido esposo José Luis Monge, personaje importante en el desarrollo de mi trabajo investigativo, quien ha sido y seguirá siendo inspiración, razón y fuerza para permanecer de pie en el continuo combate por la superación personal y profesional.

Una vez concluida la labor investigativa, se la dedico a las futuras generaciones de egresados de la carrera de Ciencias de la Ingeniería y Aplicadas, mi ferviente anhelo es: que ellos, encuentren en mi trabajo una base para continuar con el suyo, que mi investigación sirva de fuente de consulta, y sea guía, de quienes deseen extender el presente trabajo.

RESUMEN

La presente investigación versó sobre: “Auditoría Informática en la Cooperativa de Ahorro y Crédito OSCUS Ltda. Sucursal Latacunga.”, la misma que se sintetiza en los siguientes puntos:

En la parte teórica del trabajo investigativo se trato sobre Cooperativismo y Auditoría Informática con la intención de crear una visión general del terreno en el que se trabajaría, es así que es primera instancia se efectuó una visita previa a la institución a auditarse, para obtener características globales de la misma. Además en este trabajo es posible observar gráficas estadísticas que muestran la opinión de usuarios del sistema y usuarios finales sobre el sistema que emplea OSCUS.

Durante el trabajo investigativo, se recabo información sobre: el funcionamiento del sistema, el nivel de preparación informática que poseían los empleados que están directamente relacionados con los terminales de Oscus, el diseño y funcionamiento de la red, las seguridades físicas y lógicas que se emplean en la sucursal, operatividad, actualización, y características de los equipos, manuales de usuario y contingencia, inventario, etc. información que fue de vital importancia, para el desarrollo de la auditoría. Con el objetivo de formular un Informe Final de Auditoría, que contiene sugerencias sujetas a las evidencias apegadas a las normas de control para sistemas informáticos establecido en el Boletín Jurídico No 6, y las políticas del área de informática.

SUMMARY

The present investigation turned on: "Informatics Advise in the Cooperative of Saving and Credit OSCUS Ltda. Latacunga Branch." the same one that is synthesized in the following points:

In the theoretical part of the work, treats each other on Cooperation and Informatics Advise with the objective of creating a general vision of the land in the that would be worked, in first instance was effected a previous visit to the institution, for to get global characteristics of the same.

Also in this work is possible to observe graphic statistics that show the opinion of users of the system and users final on the system that employs OSCUS.

During the work, picked up information on: the information that was dealt in Oscus, the level of preparation informatics that possessed the employees that are directly related with the terminals of Oscus, the design and operation of the net, the physical securities and logics that they are employed in the branch, activity, up to date, and characteristic of the teams, manuals of user and contingency, inventory, etc. information that was from vital importance for the development of the investigation. With the objective of formulating a Report Final of Advise, that contains subject suggestions to the evidences close to the norms of control for systems informatics established in the Juridical Bulletin No 6, and the politics of the area of informatics.



NACIONAL EXPERIMENTAL
PROVINCIA DE COTOPAXI"

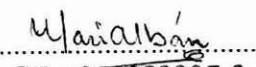
Rectorado
Pujilí-Ecuador
Tel. 723-162 723-595

CERTIFICADO

En calidad de docente del "Colegio Nacional Experimental Provincia de Cotopaxi" de la cátedra del idioma Inglés, CERTIFICO, haber leído y corregido el summary de TESIS DE GRADO denominada: "Auditoría Informática en la Cooperativa de Ahorro y Crédito OSCUS Ltda. Sucursal Latacunga" cuya autoría pertenece a la Sra. egresada Silvana del pilar Monge Herrera. En tal virtud dicho resumen está estructurado, y gramaticalmente es adecuado, en consecuencia certifico que el mencionado documento es apto para ser adjuntado a la tesis de grado.

Es todo cuanto puedo certificar en honor a la verdad, el portador del presente hará uso para los fines pertinentes.

Atentamente.


E.I. 050099907-3
Lic. María I. Albán Guano
DOCENTE

INDICE GENERAL

CAPITULO I

FUNDAMENTACION TEORICA

CONTENIDO	Pag.
Aval	ii
Responsable	iii
Informe final	iv
Dedicatoria	v
Agradecimiento	vi
Resumen	vii
Summary	viii
Introducción	ix
1.- Cooperativismo	1
1.1 Qué es una cooperativa	1
1.2 Principios del cooperativismo	1
1.3 Valores del cooperativismo	3
1.4 Como funciona una cooperativa	4
1.5 Normas de control para el área de sistemas informáticos	5
1.6 Políticas del área informática	20
1.7 Auditoría informática	21
1.7.1 Objetivos de la auditoría informática	29

1.7.2	Importancia de la auditoría informática	32
1.7.3	Necesidad de auditar	34
1.7.4	Alcance de la auditoría informática	36
1.8	Clases de auditoría informática	37
1.8.1	Auditoría informática de producción o explotación	38
1.8.2	Auditoría informática de desarrollo de proyectos	39
1.8.3	Auditoría informática de sistemas	39
1.8.4	Auditoría informática de comunicación y redes	41
1.8.5	Auditoría de la seguridad informática	41
1.8.6	Auditoría informática para aplicaciones en Internet	43
1.8.7	Auditoría de gestión	44
1.8.8	Auditoría interna	45
1.8.8.1	Ventajas de la auditoría informática interna	45
1.8.8.2	Objetivos auditoría informática interna	46
1.8.9	Auditoría informática externa	47
1.8.9.1	Ventajas de la auditoría informática externa	47
1.8.9.2	Objetivos de la auditoría informática externa	48
1.9	Técnicas de auditoría informática	48

1.9.1 Técnicas de verificación ocular	49
1.9.2 Técnicas de verificación verbal	50
1.9.3 Técnicas de verificación escrita	50
1.9.4 Técnicas de verificación documental	51
1.9.5 Técnicas de verificación física	52
1.10 Metodología de trabajo de auditoría informática	53
1.10.1 Fase I estudio preliminar	53
1.10.2 Fase II revisión y evaluación de recurso informático	55
1.10.3 Fase III examen de áreas críticas	55
1.10.4 Fase IV comunicación de resultados	58
1.11 Modelo grafico de la metodología de auditoría informática	59
1.12 Diagrama de flujo de la metodología	61
1.13 Herramientas para ejecutar auditoría informática	64
1.17 Modelo conceptual de la exposición del informe final	64
1.18 Carta de introducción o presentación del informe final	66

CAPITULO II

ANALISIS E INTERPRETACION DE RESULTADOS

2.1 Origen de oscus	67
2.2 Fundamento	68
2.3 Fines y medios	69
2.4 Objetivos, misión, visión, función de oscus	71

2.4.1 Objetivos de oscus	71
2.4.2 Misión de oscus	72
2.4.3 Visión de oscus	72
2.4.4 Función de oscus	73
2.5 Fundadores y autoridades que rigen oscus	74
2.6 Empleados de oscus y su rol dentro de la institución	75
2.7 Socios de oscus y su rol	77
2.8 Infraestructura de oscus sucursal Latacunga	78
2.9 Presentación, análisis e interpretación de resultados	79
2.9.1 Encuestas a los usuarios del sistema	79
2.9.2 Encuestas a los socios de oscus	94
2.9.3 Resultados de las entrevistas	101
2.10 Verificación de hipótesis	110

CAPITULO III

PROPUESTA

3.1 Tema	117
3.2 Objetivos	117
3.3 Justificación	118
3.4 Fundamentación	120
3.5 Presentación	121
3.6 Programa para el desarrollo de la fase I	124
3.7 Programa para el desarrollo de la fase II	126

3.8 Programa para el desarrollo de la fase III	127
3.9 Programa para el desarrollo de la fase IV	134
3.10 Informes de cumplimiento de actividades	135
3.10.1 Informe de cumplimiento de actividades de la fase I	135
3.10.2 Informe de cumplimiento de actividades de la fase II	139
3.10.3 Informe de cumplimiento de actividades de la fase III	141
3.10.3.1 Informe de tareas cumplidas del plan para evaluar sistemas ..	142
3.10.3.2 Informe de tareas cumplidas del plan para recurso humano ...	146
3.10.3.3 Informe de tareas del plan para hardware y software	147
3.10.3.4 Informe de tareas del plan para comunicaciones	148
3.10.4 Informe de cumplimiento de actividades de la fase IV	149
3.11 Análisis de la información obtenida en el cumplimiento de las tareas	150
3.11.1 Análisis de la fase I	150
3.11.2 Análisis de fase II	155
3.11.2.1 Determinación de áreas críticas	159
3.11.3 Análisis de fase III	160
3.11.3.1 Evaluación de recurso sistema	160
3.11.3.1.1 Evaluación del diseño lógico del sistema	162
3.11.3.1.2 Evaluación del desarrollo del sistema	165
3.11.3.1.3 Evaluación del control de diseño de sistemas y programación ...	168
3.11.3.1.4 Evaluaciones de la forma de implementación	169
3.11.3.1.5 Evaluación de la base de datos y código fuente	169
3.11.3.1.6 Análisis de las aplicaciones del sistema	173

3.7.3.2	Análisis de evaluación del recurso humano	179
3.7.3.3	Análisis de evaluación de hardware y software	182
3.7.3.3.1	Análisis de información obtenida con Taskinfo	182
3.7.3.4	Análisis de la red implementada en oscus	196
3.9	Carta de introducción	199
3.10	Informe final de auditoría	200

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

4.2	Conclusiones	227
4.3	Recomendaciones	229

INDICE DE TABLAS

TABLA No 1: Necesidades del usuario	79
TABLA No 2: Caídas del sistema	81
TABLA No 3: Seguridad en el manejo de la información	83
TABLA No 4: Asesoría y capacitación informática	85
TABLA No 5: Funcionamiento de la red	87
TABLA No 6: Opinión sobre el hardware y software	89
TABLA No 7: Mantenimiento de equipo	91
TABLA No 8: Sugerencias para mejorar el sistema	93
TABLA No 9: Funcionamiento del sistema	94
TABLA No 10: Atención de los empleados a los socios	96
TABLA No 11: Labores de los empleados de oscus	98
TABLA No 12: Servicio al cliente	100
TABLA No 13: Obtención del Hi cuadrado	114
TABLA No 14: Puntos críticos	115
TABLA No 15: Tabla de frecuencias	116
TABLA No 16: Programa para el desarrollo de la fase I	124
TABLA No 17: Programa para el desarrollo de la fase II	126
TABLA No 18: Programa para el desarrollo de la fase III	127
TABLA No 19: Plan para la evaluación d el sistema	128
TABLA No 20: Plan para el análisis del recurso humano	130
TABLA No 21: Plan para evaluación de hardware y software	131
TABLA No 22: Plan para evaluación de la red	133

TABLA No 23: Comunicación de resultados	134
TABLA No 24: Análisis FODA	144
TABLA No 25: Información del CPU	190
TABLA No 26: Información de sistema operativo	195
TABLA No 27: Clases de IP	196

INDICE DE FIGURAS

fig. 1.1 Principios del cooperativismo	2
fig. 1.2 Valores del cooperativismo	3
fig. 1.3 Auditoria informática	23
fig. 1.4 Objetivos de la auditoria informática	32
fig. 1.5 Seguridad informática	42
fig. 2.1: Necesidades del empleado, con respecto al sistema	79
fig. 2.2: Caídas del sistema.	81
fig. 2.3: Seguridad en el manejo de la información.	83
fig. 2.4: Asesoría y capacitación informática.	85
fig. 2.5: Funcionamiento de la red	87
fig. 2.6: Opinión sobre hardware y software	89
fig. 2.7: Mantenimiento de equipos	91
fig. 2.8: Sugerencia para mejorar el sistema	93
fig. 2.9: Funcionamiento del sistema	94
fig. 2.10: Atención al cliente	96
fig. 2.11: Labores de empleados en oscus	98

fig. 2.12: Servicio al cliente	100
fig. 2.13 Punto crítico de X^2	116
fig. 3.1 Código de colores	199

INDICE DE ANEXOS

ANEXO No 1: Comunicación de inicio de examen	CD
ANEXO No 2: Modelo de las hojas de trabajo	CD
ANEXO No 3: Ubicación geográfica de Oscus Sucursal Latacunga ...	CD
ANEXO No 4: Entrevista realizada al gerente de la sucursal	232
ANEXO No 5: Estructura organizacional Sucursal Latacunga	CD
ANEXO No 6: Entrevista realizada jefe del área informática	234
ANEXO No 7: Ubicación geográfica de la Matriz OSCUS	CD
ANEXO No 8: Estructura organizacional y funcional del área informática ...	CD
ANEXO No 9: Guía de visita previa	CD
ANEXO No 10: Cuestionario de control interno	CD
ANEXO No 11: Carta a gerencia	CD
ANEXO No 12: Plan estratégico para cumplimiento de fase III	CD
ANEXO No 13: Test de Auditoría de Sistemas	CD
ANEXO No 14: Encuesta a los usuarios del sistema	236
ANEXO No 15: Ejemplo de restricción de acceso a aplicaciones	CD
ANEXO No 16: Currículo Vitae	CD
ANEXO No 17: Modelo de sello adhesivo	CD
ANEXO No 18: Modelo de certificación	CD

ANEXO No 19: Información obtenida con TaskInfo	CD
ANEXO No 25: Inventario hardware y software	CD
ANEXO No 26: Red implementada en Oscus	CD
ANEXO No 27: Resultados del software Network Inspector	CD
ANEXO No 28: Información obtenida con PRTG Traffic	CD
ANEXO No 29: Información obtenida con ETHERREAL	CD
ANEXO No 30: Grafica de la red	CD
ANEXO No 31: Ubicación de las máquinas en la Sucursal	CD
ANEXO No 32: Ubicación del equipo en el área informática	CD
ANEXO No 33: Hojas de hallazgos	CD
ANEXO No 34: Carta de introducción	CD
ANEXO No 35: Anteproyecto de tesis	CD

CAPITULO I

FUNDAMENTACION TEORICA

INTRODUCCION

En el umbral del nuevo milenio, la informática es considerada como una herramienta principal en todas las áreas del desarrollo socio-económico del país, por lo que el propósito de esta investigación es establecer una Auditoría Informática en la Cooperativa de Ahorro y Crédito OSCUS Ltda. Sucursal Latacunga.

Debido al avance tecnológico, y a la incursión de todas las entidades del sistema financiero nacional, es de vital importancia la necesidad de auditar a la Cooperativa OSCUS Sucursal Latacunga, en la aplicación de la informática en todos los campos, lo que corrobora la necesidad de una buena utilización de los recursos informáticos.

En la investigación previa se determino varios aspectos como el tipo de información, la calidad del talento humano informático, el funcionamiento en red de las máquinas, nivel de seguridad; y otros, cuyos datos contribuyen a la estructuración del informe final en el que se plasmarán los hallazgos, sugerencias y recomendaciones, para mejorar la utilización de los recursos informáticos.

Al implantar la Auditoría Informática se deducirá la importancia que la Cooperativa OSCUS se inserte en la era de la automatización, es así que quien examina con prioridad su empresa, tendrá una visión del estado real de su

organización, estableciendo mecanismos para una administración eficiente, hacia el logro de un servicio eficaz, que satisfaga las necesidades del cliente o socio, razón por demás obvia para efectuar una auditoría que arroje resultados apegados a datos verídicos sujetos a comprobación, proyectándose hacia la calidad y excelencia de los servicios.

CAPITULO I

FUNDAMENTACION TEORICA

COOPERATIVISMO

1.- COOPERATIVISMO

1.1 ¿Qué es una Cooperativa?

De acuerdo con la definición que hace la Ley de Cooperativas de la Comunidad de Madrid: " la Cooperativa es una asociación autónoma de personas y entidades que se han unido de forma voluntaria para satisfacer sus necesidades y aspiraciones económicas y sociales en común, mediante una empresa de propiedad conjunta y de gestión democrática".

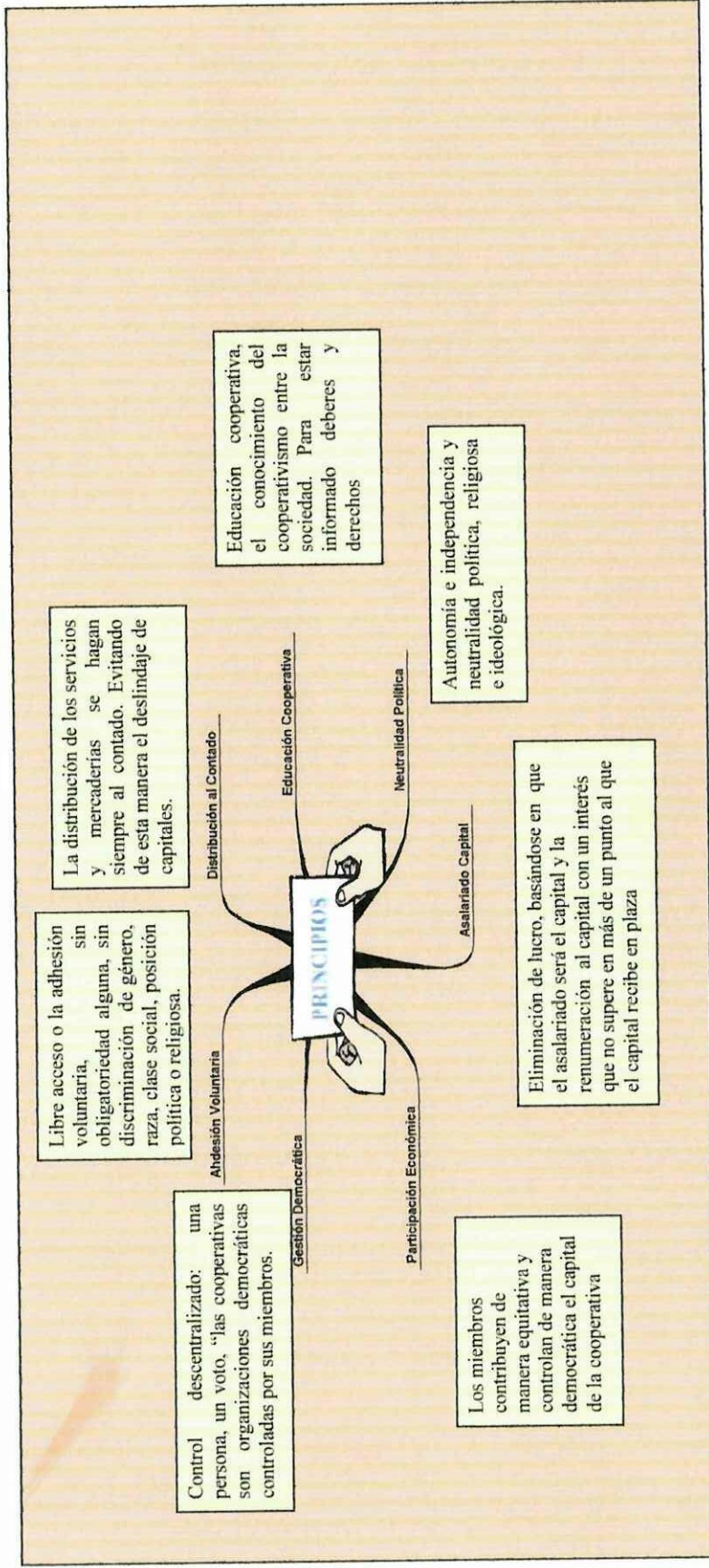
Al formar una cooperativa el objetivo principal es servir a los demás, es decir que podemos definir a la cooperativa como una entidad basada en el común bienestar.

1.2 RINCIPIOS DEL COOPERATIVISMO

Los principios son una serie de fundamentos que de ser eficazmente aplicados, permiten establecer y mantener un óptimo clima laboral. El cooperativismo se basa en ciertos principios que regulan su funcionamiento pudiendo ser estos:

A continuación se puede observar un resumen de los principios del Cooperativismo.

Fig. 1.1 PRINCIPIOS DEL COOPERATIVISMO

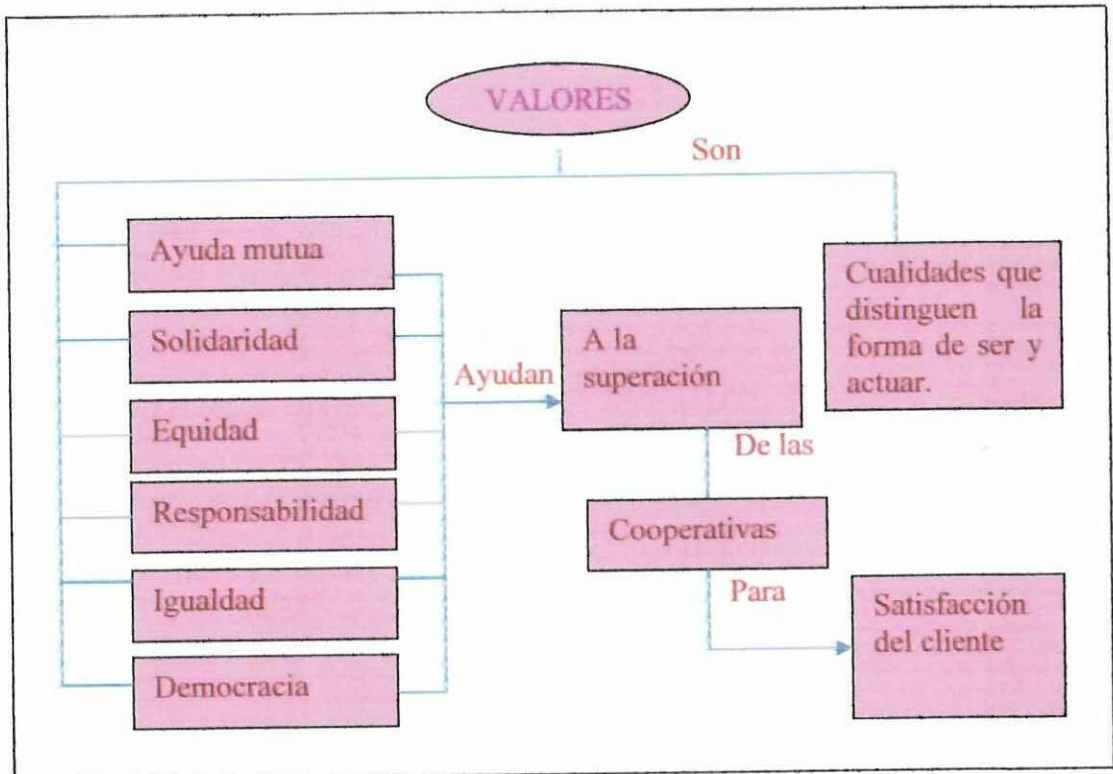


FUENTE: Texto anterior
REALIZADO POR: Investigador

1.3 VALORES DEL COOPERATIVISMO

En la igualdad los miembros de la cooperativa tienen los mismos derechos sin distinción; en la democracia los socios participan tomando decisiones, votando y trabajando conjuntamente, en la responsabilidad los miembros promocionan su cooperativa y su funcionamiento, con la ayuda mutua el desarrollo se logra en unión, trabajando para un mismo fin, con la solidaridad se mantienen juntos luchando para una mejor calidad de vida, en la equidad el justo trato de miembros, y las ganancias distribuidas de acuerdo a la participación activa.

Fig. 1.2 VALORES DEL COOPERATIVISMO



FUENTE: Texto anterior
REALIZADO POR: Silvana Monge

1.4 ¿CÓMO FUNCIONA UNA COOPERATIVA?

Las cooperativas se organizan en función de sus asociados, por lo tanto el órgano máximo es la Asamblea de Asociados, la cual representa la voluntad colectiva de sus miembros, le sigue el Consejo de Administración el cual tiene por función atender al bienestar general de la entidad y aplicar las políticas que se aprobaron en la asamblea.

Otro órgano social, es la sindicatura, que también esta integrada por asociados elegidos en asamblea, éste órgano tiene por función vigilar que no se lesionen los derechos de los asociados.

Se admite en diversos casos la realización de operaciones de las cooperativas con no asociados, hay usuarios que no son asociados. Por otra parte se, admite, generalmente y salvo determinados casos, la existencia absoluta de asociados y usuarios que no utilizan o sólo utilizan raramente los servicios de la cooperativa; y ello también se opone a la aludida identificación absoluta de los caracteres de asociados y usuarios de las cooperativas

La realización de operaciones con no asociados ya fue doctrinariamente aconsejada por autores como Charles GIDE o Ernest POISSON; y, en la práctica, ella se admite en un creciente número de países, con el objeto de consolidar esas

entidades mediante un incremento en el volumen de sus operaciones y como forma de atraer hacia el movimiento cooperativo a futuros asociados.

1.5 NORMAS DE CONTROL PARA EL AREA DE SISTEMAS INFORMÁTICOS

400 – 00 AREA: NORMAS DE CONTROL INTERNO PARA EL ÁREA DE
SISTEMAS DE INFORMACIÓN COMPUTARIZADOS

400 – 01 TITULO: ORGANIZACIÓN DEL ÁREA INFORMÁTICA

400 - 01 TITULO: ORGANIZACIÓN DEL ÁREA INFORMÁTICA

Cada entidad establecerá los lineamientos que orienten el proceso de organización del área de informática, aspecto que implica la definición de actividades a cumplir, las funciones y responsabilidades del personal, al igual que las interrelaciones de los elementos comprendidos en este sector con las áreas operativas de la entidad, Estos elementos formarán parte del Manual de Organización y Funciones, correspondiente.

La estructura básica del área de Informática estará constituida por áreas que son importantes para el funcionamiento, de acuerdo a las necesidades de cada entidad.

Corresponde a la máxima autoridad de la entidad aprobar las políticas que permitan organizar apropiadamente al área de informática y asignar los recursos humanos calificados y equipos de computación necesarios.

**400 – 02 TITULO: PLAN INFORMÁTICO, ADQUISICIÓN O
ACTUALIZACIÓN DE SISTEMAS**

Los sistemas de información computarizados se generan de acuerdo a los requerimientos o necesidades establecidas en cada entidad del sector público, y será necesario que la máxima autoridad apruebe un **PLAN INTEGRAL INFORMÁTICO**, con sujeción a las disposiciones vigentes. Dicho plan será de carácter obligatorio, independiente del nivel de complejidad o tamaño de la entidad, además será el que regule y determine el desarrollo informático de la institución a corto y mediano plazo.

El plan Integral debe contener lo siguiente:

1. Fase organizacional referente a la misión de la entidad, estructura orgánica, ANÁLISIS FODA situación actual del área informática en: recursos humanos, HARDWARE y SOFTWARE.
2. La definición de los Sistemas de Información Computarizados que necesita la institución.
3. La priorización de los mismos

4. La base tecnológica requerida para su implantación
5. El presupuesto financiero.
6. Plan de inversiones; y,
7. El cronograma de las actividades principales a desarrollar para la ejecución del plan.

Esa metodología incorporará en todas sus fases, la participación de los usuarios y de la Unidad de Auditoría Interna, donde ésta exista, así como instancias de aprobación y aceptación escritas por parte de los usuarios directamente involucrados y la entrega obligatoria de la documentación detallada de cada fase, del sistema en general y de su operación o del usuario.

En caso de adquisición de programas de computación (paquetes de software) se preverán tanto en el proceso como en los contratos respectivos, mecanismos que aseguren el cumplimiento satisfactorio de los requerimientos de la entidad, la obtención de la licencia de uso legalizada, la recepción de los programas, diseños, documentación en general y la garantía de mantenimiento ofrecida por el proveedor.

En la adquisición de equipos de computación (hardware), los contratos respectivos, tendrán el detalle suficiente que permita establecer la marea y las características técnicas de los principales componentes al igual que la garantía ofrecida por el proveedor, a fin de determinar la correspondencia de los equipos

adquiridos con los requerimientos establecidos en el proceso de contratación, lo que quedará confirmado en las actas de entrega / recepción. Para la incorporación de nuevos sistemas y para la actualización o crecimiento de los existentes, se utilizará tecnología probada y actual tanto en los equipos como en los programas de computación de soporte (software de base). El proceso de desarrollo de sistemas seguirá una metodología que comprenda al menos:

1. Un análisis de factibilidad;
2. Una propuesta de desarrollo;
3. Un diseño conceptual y físico;
4. Una prueba de aceptación luego de una etapa de trabajo en paralelo;
5. Un plan de implantación que considere:
 - Capacitación
 - Adecuación de los nuevos sistemas
 - Mantenimiento

400 - 03 TITULO: OPERACIÓN Y MANTENIMIENTO

Para los sistemas incorporados a su gestión, en cada entidad se elaborarán procedimientos formales y detallados del funcionamiento y operación, tanto a nivel de usuarios como de la unidad de sistemas de información computarizados.

Los sistemas en operación se someterán a constantes pruebas y evaluaciones para identificar inconsistencias o inconformidades respecto a su funcionamiento. Para solucionar estas deficiencias aplicarán los procedimientos de mantenimiento de los sistemas, los mismos que serán definidos por la entidad.

Para el mantenimiento de sistemas, la entidad contará con mecanismos documentados de los cambios y ajustes efectuados.

400 - 04 TITULO: ACCESO A LOS SISTEMAS Y MODIFICACIÓN DE LA INFORMACIÓN

La máxima autoridad de cada entidad pública o por su delegación los directivos y jefes de unidad administrativa, en coordinación con el jefe de la Unidad de Procesamiento Automático de Datos, establecerán las medidas que permitan acceder y modificar los datos e información contenidos en los sistemas computarizados solo a personal autorizado. Estas se concretarán en controles de acceso físico y lógico.

Entre los controles de acceso físico a los puntos terminales del sistema de información computarizado se tomarán en cuenta los siguientes:

1. Mantener los puntos terminales bajo llave;
2. Mantener los puntos terminales bajo supervisión directa; y,
3. Utilizar llaves para operar los puntos terminales.

Entre los controles de acceso lógico a los sistemas y la información contenida en la computadora, se utilizará:

1. Claves de accesos (palabras secretas);
2. Rangos limitados de actividades (menús restringidos);
3. Perfiles de acceso, de acuerdo a las funciones y jerarquías de los usuarios; y,
4. Una bitácora de operación de los sistemas llevada en forma manual o computarizada, la misma que consistirá en al menos:
 - Un registro de utilización de cada uno de los sistemas por cada uno de los usuarios;
 - Registro de los intentos de acceso no autorizados; e,
 - Implantación de circuitos especiales que identifican al dispositivo terminal como autorizado para acceder a los sistemas.

Se entenderá por "puntos terminales" a las terminales de computación, los microcomputadores independientes y los conectados a otros equipos, ya sea en la modalidad de red o multiusuario, y todos aquellos dispositivos que permitan la intercomunicación directa del usuario con el computador.

400 - 05 TITULO: ENTRADA Y SALIDA DE DATOS

Deben diseñarse controles con el propósito de salvaguardar los datos fuente, las operaciones de proceso y salida de información, con la finalidad de preservar la integridad de la información procesada por la entidad.

Para implementar los controles sobre datos fuente, es necesario que la entidad designe a los usuarios encargados de salvaguardar los datos. Para ello, deben establecerse políticas que definan las claves de acceso para los tres niveles:

- Primer nivel: Únicamente tiene opción de consulta de datos;
- Segundo nivel: Captura, modifica y consulta datos; y,
- Tercer nivel: Captura, modifica, consulta y además puede realizar bajas de datos.

Los controles de salida de datos protegerán la integridad de la información, para cuyo efecto es necesario tener en cuenta aspectos tales como:

- Copias de la información en unidades;
- La identificación de las personas que entregan el documento de salida; y,
- La definición de las personas que reciben la información.

Los controles de operación de los equipos de cómputo están dados por procedimientos estandarizados y formales que se efectivizan de la siguiente forma:

- Describen en forma clara y detallada los procedimientos;
- Actualizan periódicamente los procedimientos; y,
- Asignan los trabajos con niveles efectivos de utilización de equipos.

En tal razón, los jefes de las unidades administrativas, serán responsables de asegurar que los sistemas tengan controles, sean éstos manuales o automáticos de validación de los datos que van a ser ingresados al computador, puntualizando en los procedimientos para verificar que la información registrada en los documentos fuente es correcta, es decir, permitan identificar los errores y efectuar los ajustes que sean necesarios en el proceso.

Se aplicarán procedimientos que garanticen el ingreso al computador de datos validos, es decir, que sean consistentes con los archivos.

Corresponde a la Dirección de la entidad, en coordinación con el Área de Informática, establecer los controles de datos fuente, los controles de operación y los controles de seguridad, con el objeto de asegurar la integridad y adecuado uso de la información que produce la entidad.

400 - 07 TITULO: PROCESAMIENTO Y ENTREGA DE DATOS

La máxima autoridad de cada entidad pública o por su delegación los jefes de las unidades administrativas, establecerán controles en los sistemas de información para asegurar que los datos procesados y la información obtenida sean completos y correspondan al período correcto, estos controles podían ser manuales o automáticos, según la información procesada, y consistirán en:

1. Totalización de valores críticos, antes y después del procesamiento;
2. Verificación de compatibilidad de fechas y transacciones y modificaciones.
3. Balanceo de saldos o totales de conciliación;
4. Utilización correcta de archivos para procesamiento;
5. Verificar que los datos transmitidos hayan sido completos;
6. Consistencia en la recuperación de transacciones, luego de una interrupción;
7. Validez de datos generados automáticamente; y,
8. Generar rastro o pistas de auditoría.

La información procesada será entregada de forma oportuna y completa a los usuarios autorizados, dejando constancia escrita de esta entrega.

400 – 08 TITULO: SEGREGACIÓN DE FUNCIONES EN EL ÁREA DE INFORMÁTICA

La máxima autoridad de una entidad del sector público, será la encargada de definir las funciones de la unidad de Procesamiento Automático de Datos.

Esta segregación de funciones será definida en la estructura orgánica y se especificará las responsabilidades individuales de los usuarios internos de cada servidor; así como también definirá la estructura jerárquica necesaria para el adecuado funcionamiento de los Sistemas de Información Computarizados en lo que corresponde a la dirección, supervisión y operación de la parte técnica y al enlace entre las unidades de sistemas de información Computarizados y sus usuarios.

Fue el caso de los sistemas que funcionen independientemente de la Unidad de Procesamiento Automático de Datos o en aquellas actividades que debido a su tamaño no disponen de una unidad de sistemas, se compensará la falta de segregación de funciones incorporando controles por parte del usuario, siendo el jefe o responsable del área el que debe implementar dichos controles, que, entre otros, pueden ser:

- Supervisar directamente la utilización y seguridad de los sistemas;
- Mantener registros por tipo de transacción;

- Obtener totales de control de datos permanentes;
- Conciliar los datos ingresados con la información de salida; y,
- Revisar los datos de entrada y salida considerados significativos.

Para garantizar la contabilidad de las operaciones de la Unidad de Procesamiento Automático de Datos se mantendrá una división funcional que permita segregar la administración de la unidad, el desarrollo de sistemas.

Por unidad de Procesamiento Automático de datos se entenderá al área responsable de desarrollar, actualizar y operar los sistemas computarizados, a nivel de toda la institución o de una parte de ella.

400 - 09 TITULO: SEGURIDAD GENERAL EN LOS CENTROS DE PROCESAMIENTO DE DATOS

Los centros de procesamiento de datos de la institución, establecerán mecanismos que protejan y, salvaguarden contra pérdidas y fugas de los medios físicos (equipos y programas) y la información. Con este fin aplicarán por lo menos las siguientes medidas:

1. Procedimientos de acceso físico restringido al centro de procesamiento de datos, biblioteca magnética, documentos, datos y documentación de los programas;

2. Obtención periódica de respaldos y ubicación física de los más importantes en lugares resguardados, fuera de los centros de procesamiento de datos;
3. Seguridades e instalaciones físicas adecuadas;
4. Un plan de contingencias que prevea las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas con los equipos, con los programas o con el personal; el Plan de Contingencias abarcará los siguientes aspectos:

1. Plan de reducción de riesgos (Plan de seguridad)
2. Plan de recuperación de desastres:

- Actividades previas al desastre
- Actividades durante el desastre (Plan de emergencias, entrenamiento)
- Actividades después del desastre.

El plan de contingencias es un documento de carácter confidencial que describe los procedimientos que debe seguir la oficina de informática para actuar en caso de una emergencia que interrumpa la operatividad del sistema de cómputo.

La aplicación del plan permite operar en un nivel aceptable cuando las facilidades de procesamiento de información no están disponibles.

El plan de contingencias aprobado, se distribuye entre el personal responsable de su operación. La revisión del plan debe realizarse cuando se haya efectuado algún cambio en la configuración de los equipos.

Corresponde al área de informática elaborar, mantener y actualizar el Plan de Contingencias, a fin de asegurar el funcionamiento de los sistemas de información que requiere la entidad para el desarrollo de sus actividades.

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

Se entenderá por centro de procesamiento de datos al área física donde se ubica a los computadores que almacenan la información.

400 - 10 TITULO: UTILIZACIÓN DE LOS EQUIPOS, PROGRAMAS E INFORMACIÓN INSTITUCIONAL

La máxima autoridad de cada entidad pública o por su delegación los directivos y jefes de las unidades administrativas, establecerán procedimientos para asegurar el uso eficiente, eficaz y económico de los equipos, programas de computación e información computarizada, a través de:

1. El registro y seguimiento de la operación de los mismos;

2. La capacitación de funcionarios en la utilización de los equipos y programas;
- y,
3. La evaluación periódica de los objetivos cumplidos mediante la computarización.

Los equipos y programas serán utilizados exclusivamente en las actividades propias de la institución.

La información obtenida del proceso computarizado será de uso e intercambio entre las instituciones del sector público, con excepción de aquella considerada expresamente como reservada o de uso restringido.

En el caso de fijarse un valor para la información a proporcionar a estas entidades, el mismo considerará únicamente los costos de su obtención, procesamiento y transmisión que será materia del reglamento pertinente.

400 - 11 TITULO: APROVECHAMIENTO DE LOS RECURSOS COMPUTARIZADOS

La máxima autoridad de cada entidad pública establecerá mecanismos que aseguren eficiencia, efectividad y economía en el aprovechamiento de los recursos computarizados (equipos, programas e información) del sector público.

Estos mecanismos promoverán y viabilizarán el intercambio de información interinstitucional así como de programas de aplicación desarrollados al interior de las instituciones.

Complementariamente, el organismo competente autorizará la adquisición de bienes y servicios para sistemas computarizados, tomando en cuenta la "compatibilidad" tanto en equipos como en programas que permita la interconexión de los sistemas y mantendrá un registro del Parque Informático del Sector Público. Esta última información será difundida periódicamente a las instituciones interesadas, a nivel nacional.

Cada entidad pública mantendrá un registro de los equipos y programas que posee, para que puedan ser considerados en el Parque Informático del Sector Público.

El Parque Informático del Sector Público estará conformado por las sumas de los equipos, programas e información computarizados (software y hardware) que posean las entidades gubernamentales.

1.6 POLITICAS QUE REGULAN EL FUNCIONAMIENTO DEL ÁREA INFORMATICA DE OSCUS

- Política para la liberación y respaldo de la información de la Base de Datos
- Política para la seguridad física y control de acceso al área de procesamiento
- Política para la seguridad física del personal y equipos
- Política para el uso y restricción de acceso restringido a quipos.
- Política para la capacitación del personal de informática y afines
- Política de actualización de versión del aplicativo y Base de Datos
- Política de usuarios y claves confidenciales
- Política para el mantenimiento de hardware, software y sistema
- Política para la seguridad física y de acceso a los centros de acopio y procesamiento de datos
- Política de entrenamiento para el entrenamiento y/o modificaciones del aplicativo

En una institución financiera como los son las cooperativas, que emplean computadores, procesos automatizados, comunicaciones en red, etc. el buen funcionamiento de estos depende de la evaluación periódica del estado de los equipos, del sistema, en este caso la aplicación de auditoría informática es un aliado para la detección temprana de errores, por lo tanto se presenta la definición de auditoría informática:

1.7 AUDITORÍA INFORMÁTICA

No existen definiciones oficiales sobre ¿qué es la Auditoría Informática?, y algunas de las que aparecen en libros o se dan en cursos y seminarios tienen la influencia y criterio personal de su autor, no obstante, a continuación mencionamos las que se consideran más importantes:

De acuerdo con la pagina www.monografias.com/auditoriainformatica/conceptos.com **AUDITORÍA INFORMÁTICA** es: "Es el conjunto de técnicas, actividades y procedimientos, destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control eficacia, seguridad y adecuación del servicio informático en la empresa, por lo que comprende un examen metódico, puntual y discontinuo del servicio informático, con vistas a mejorar en: Rentabilidad, Seguridad, Eficacia."

www.monografias.com/auditoriainformatica/conceptodeauditoríadesistemasdeinformación; muestra que **AUDITORÍA INFORMÁTICA** es: "la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones"

Para CATAFORA, Carpio Fernando,(1.998) Manual de Auditoría Informática, Especialista en Sistemas de Información Gerencial y profesor de esta cátedra en la Universidad Católica Andrés Bello de Caracas, Venezuela, dice que **AUDITORÍA INFORMÁTICA** es: "La Auditoría Informática es aquella que tiene como objetivo principal la evaluación de los controles internos en el área de PED (Procesamiento Electrónico de Datos).

En concordancia con las citas anteriores la Auditoría Informática es aquella que tiene como objetivos evaluar, verificar y recomendar los controles de la función informática, en todo el campo informático o en un área específica; se ejecuta Auditoría Informática con miras a analizar la eficiencia de los sistemas, verificar el cumplimiento de las políticas y procedimientos de la empresa en este ámbito y revisar que los recursos materiales y humanos de esta área se utilicen eficientemente. El auditor informático debe velar por la correcta utilización de los recursos que la empresa dispone para lograr un eficiente y eficaz Sistema de Información.

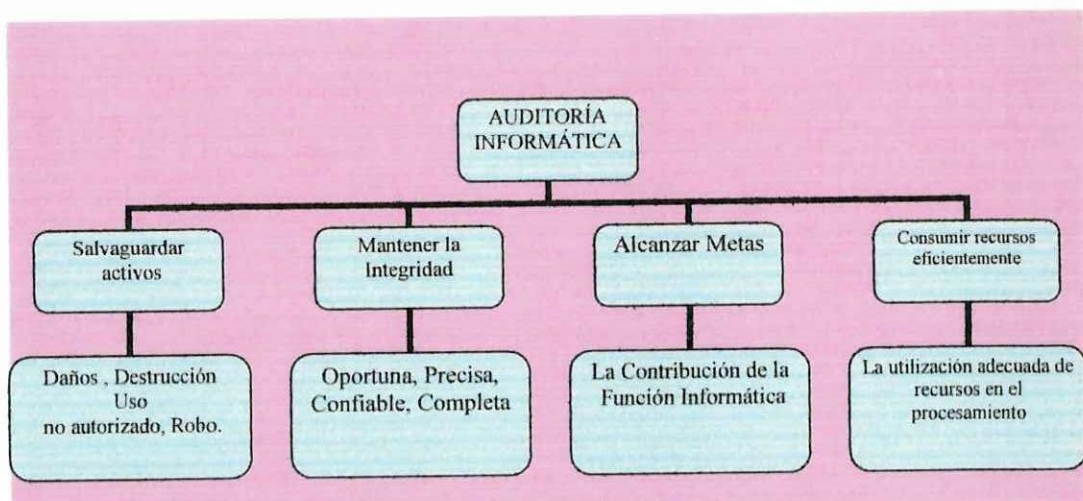
La Auditoría Informática comprende la revisión y la evaluación independiente y objetiva, por parte de personas competentes. Los auditores que incursionan en el entorno informático de una entidad, deben poseer conocimientos sobre informática, para cumplir con: objetivos fijados, contratos y normas legales aplicables.

La auditoría Informática es un examen especial encaminado a examinar secciones o todo el entorno informático de una empresa con el objetivo primordial de obtener conclusiones que leven a emitir sugerencias que ayuden al mejoramiento del estado informático dentro de una entidad.

De forma sencilla en la siguiente figura, se muestra a la Auditoría Informática como el proceso de recolección y evaluación de evidencia para determinar el buen o mal funcionamiento de la entidad auditada: Así pues, se reafirma que la Auditoría Informática, conocida en como Auditoría de Sistemas, nace en nuestro medio en base a que la información es el activo más importante de las empresas.

En la siguiente gráfica se muestra los tópicos que se pretenden lograr con la aplicación de auditoría informática.

Fig. 1.3 AUDITORIA INFORMATICA



FUENTE: Páginas de Internet
AUTOR: Silvana Monge

Al aplicar Auditoría Informática, es posible efectuar un examen de lo que acontece realmente en los Sistemas de Información se puede determinar los pasos del proceso intermedio de la introducción de datos al sistema y la obtención de resultados.

Según el ingeniero diplomado CASTRO, Julián, (2003) Manual de Auditoría Informática, **AUDITORÍA INFORMÁTICA** es: “La verificación de controles en el procesamiento de la información, instalaciones, con el objeto de evaluarlos y presentar recomendaciones a gerencia” (Pg. 17)

De acuerdo MAZZAL Miguel, (2001) El mundo de la Auditoría Informática, **AUDITORÍA INFORMÁTICA** es: “La actividad dirigida a verificar y juzgar información”, (Pg. 19)

Según RIOS, Wellintong, (2000) Auditoría Informática Guía Para su Aplicación, **AUDITORÍA INFORMÁTICA** es: “El examen de los procesos del área de procesamiento de datos, y la utilización de los recursos que en ellos intervienen para llegar a establecer conclusiones y recomendaciones encaminadas a corregir deficiencias existentes”. (Pg. 17)

En concordancia con los autores de las citas anteriores Auditoría Informática es un examen especial dirigido a un sector específico como es el informático, puesto que es la verificación del funcionamiento no de toda la institución sino de una de

sus funciones, en este caso del tratamiento automático de la información, con el objetivo de examinar los procesos, el tratamiento, aprovechamiento de los recursos informáticos disponibles, para determinar fallas o aciertos existentes y generar conclusiones que conlleven a sugerir mejoras, encaminadas a corregir deficiencias que quizá estén amenazando seriamente al buen funcionamiento el área informático y por lo tanto de la institución, la cual depende del acierto en las sunciones informáticas para lograr la satisfacción del cliente.

La Auditoría Financiera es limitada en cuanto a la revisión del recurso informático quizá podría analizar los costos de obtención de equipo o software, pero nada más, en tanto que la Auditoría Informática revisa y la evalúa los seguridades físicas/lógicas, procedimientos de informática; etc.

La auditoría de recurso informático es extensa, por tanto existe la posibilidad de auditar cada aspecto por separado, por ejemplo, comunicación y redes; funcionamiento, administración de usuarios etc. del sistema, funcionamiento, actualización, utilización, etc. de los equipos de computo. De este modo el examen sería más específico, centralizándolo en áreas pequeñas y con mejores resultados.

Al ejecutar auditoria, el responsable prepara una serie de cuestionarios llamados Check List, los cuales tienen que ser comprendidos por el auditor al pie de la letra, puesto que si son mal aplicados y mal recopilados, pueden generar resultados

distintos a los esperados. Este es uno de tantos instrumentos existentes para obtener información, como ya se verá más adelante.

Como se observa en la página de Internet http://html.rincondelvago.com/auditoria-informatica_1.html de GREER Richard, del 28/11/05 **AUDITORÍA INFORMÁTICA** es: “La Auditoría informática esta basada en la palabra auditor que viene del griego auditorius que significa virtud de oír”

Así mismo en la página <http://www.odec.es/odec/index.php?id=717> de REYES Miguel, 17/11/05, podemos observar que la **AUDITORIA INFORMÁTICA** es: “La auditoría informática es la revisión de los sistemas de información actuales, tanto a nivel hardware como software, con objeto de descubrir potenciales puntos de mejora y determinar en qué modo debería actuarse para mejorar tanto éstos como otros aspectos.

En la página <http://www.monografias.com/trabajos5/audi/audi.shtml> de LAMBERT Anthony, 25/11/05 **AUDITORÍA INFORMÁTICA** es: revisión de todos los procesos encargados de producir resultados, entre ellos la captura de la información, los sistemas hardware de explotación, los recursos humanos de explotación y otros.

De acuerdo con la página http://www.auditoriasistemas.com/auditoria_informatica.htm, de RUIZ Angelina, 14/10/05 la **AUDITORÍA INFORMÁTICA**. La Auditoría Informática es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una empresa.

En <http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml> de CORRALES Lourdes, 27/10/05, manifiesta que **AUDITORIA INFORMÁTICA** es: “Es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una sección, un organismo, una entidad, etc.”

Por otra parte, el diccionario Español Sopena define a la **AUDITORIA INFORMATICA** como: “Revisor de Cuentas colegiado. En un principio esta definición carece de la explicación del objetivo fundamental que persigue todo auditor: evaluar la eficiencia y eficacia.” (Pg. 24)

Según RAMOS Gonzales, en <http://www.monografias.com/trabajos22/auditoria-informatica/auditoria-informatica.shtml#concep>, 14/10/05 "La **AUDITORÍA INFORMÁTICA** es: “comprende la revisión y la evaluación independiente y objetiva, por parte de personas independientes y técnicamente competentes del entorno informático de una entidad.”

De acuerdo con la página <http://dmi.uib.es/~bbuades/auditoria/tsld004.htm>, de VESSARE, Laura 28/10/05, **AUDITORÍA INFORMÁTICA** es: “Actividad para

determinar, por medio de la investigación, la adecuación de los procedimientos establecidos, instrucciones, especificaciones.

En la página <http://dmi.uib.es/~bbuades/auditoria/sld003.htm>, de CHIOOP, Hernest, 24/10/05, Podemos ver que **AUDITORIA INFORMATICA** es: “Examen metódico de una situación relativa de un producto, proceso u organización, en materia de calidad, realizado en cooperación con los interesados, para verificar la concordancia de la realidad con lo preestablecido y la adecuación al objeto buscado”.

En http://ciberia.ya.com//auditoria_informatica.htm#Auditoría%20Informática, de CHEYENNE, Homero, 10/10/05 **AUDITORIA INFORMATICA** es: “la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información”

Para poder ejecutar Auditoría Informática se deben cumplir algunos requisitos como:

- Seguir una metodología preestablecida,
- Realizar en una fecha precisa y fija y
- Será personal extraño al servicio de informática.

Para finalizar se concluye que la Auditoría Informática es la encargada de vigilar y evaluar, el recurso informático disponible en la institución a auditarse,

basándose en la imparcialidad, para emitir un juicio global o parcial fundamentado en hechos y situaciones indiscutibles, teniendo la plena capacidad de dar sugerencias cristalizadas en el informe final; pero careciendo de poder para modificar la situación analizada por él mismo, únicamente los directivos de la empresa tienen la última palabra.

1.7.1 OBJETIVOS DE LA AUDITORÍA INFORMÁTICA

El objetivo primordial de la Auditoría Informática es: evaluar la eficiencia y eficacia del ámbito informático.

Como Objetivos generales de la Auditoría de sistemas informáticos podemos nombrar los siguientes:

- Evaluación de los sistemas y procedimientos.
- Evaluación de los equipos de cómputo.
- Examinar la seguridad del personal, los datos, el hardware, el software y las instalaciones.
- Justipreciar la reducción de riesgos en el uso de Tecnología de información
- Constatar la seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático.
- Analizar la eficacia del Sistema Informático.

Los objetivos que se citaron anteriormente tienen estrecha relación la creciente expansión de ordenadores es decir que ellos se interconectan entre sí, los sistemas se articulan y generan complejas redes y organizaciones informáticas que manejan grandes y complejos recursos, lo cual representa un reto para la Auditoría Informática al tratar de analizar, hallar conclusiones razonadas, descubrir fortalezas y debilidades y expresar juicios objetivos sobre un conjunto de aspectos muy complejos cuyo soporte son las tecnologías informáticas, y los Sistemas de Información.

Otro de los objetivos que son base fundamental de la Auditoría Informática es la vigilancia de la operatividad, teniendo en cuenta que esta operatividad se relaciona íntimamente con la de eficacia, eficiencia, confiabilidad e integridad de los recursos informáticos.

Si hablamos que operatividad significa buen funcionamiento de la maquinaria entonces este punto se convierte en la principal preocupación del auditor informático y uno de los primordiales objetivos del examen auditor; para conseguir deslindar posibles fallas en este aspecto, el auditor se sirve de Controles Técnicos Generales de Operatividad y Controles Técnicos Específicos de Operatividad, que a continuación se presentan con mayor detalle para mostrarnos la importancia de Auditar y los problemas que acarrea la inoperatividad.

- Los Controles Técnicos Generales son los que se realizan para verificar la compatibilidad de funcionamiento simultáneo del Sistema Operativo y el Software de base con todos los subsistemas existentes, así como la compatibilidad del Hardware y del Software instalados.

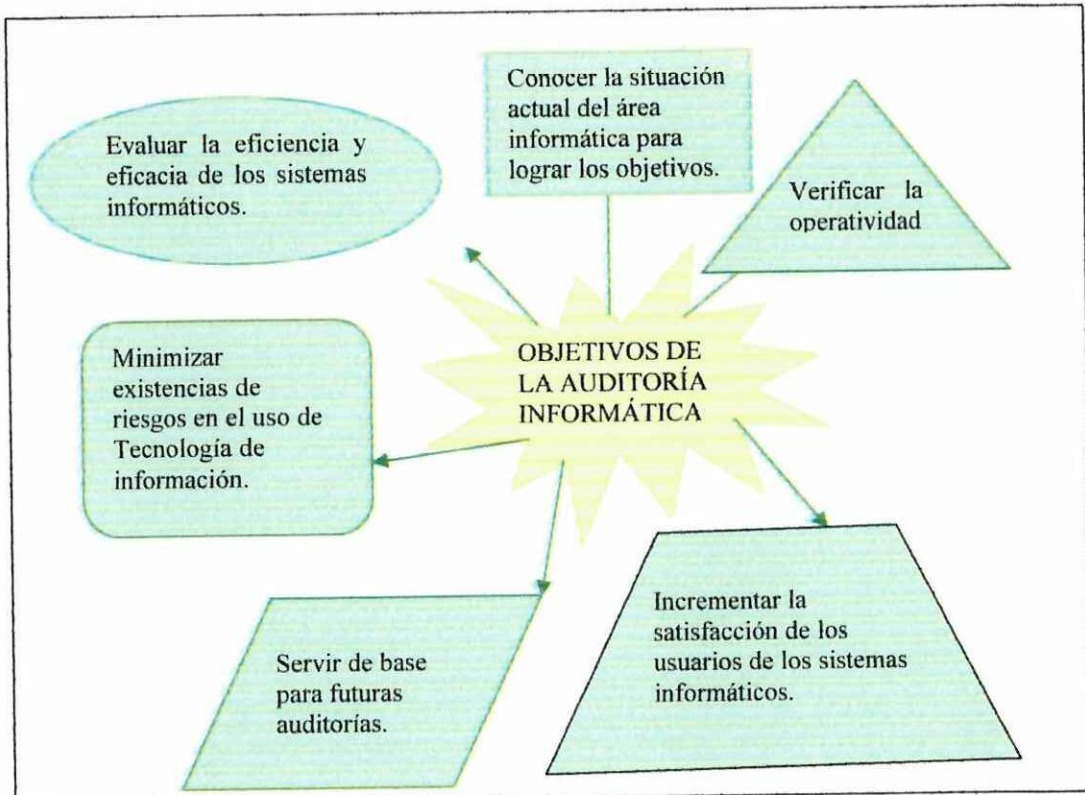
En la actualidad las redes informáticas tienen gran amplitud geográfica lo que hace que los empresarios contraten diversos productos de Software básico, con el consiguiente riesgo de que cada Centro de Proceso de Datos, intercomunicación de todos los Centros de Proceso de Datos si no existen productos comunes y compatibles.

- Los Controles Técnicos Específicos, son igualmente necesarios para lograr la Operatividad de los Sistemas.

En conclusión, el objetivo medular de la Auditoría Informática, es evaluar la actividad del recurso informático, determinar causales de mal funcionamiento, en el caso de detectarse y emitir posibles soluciones.

En la siguiente figura se muestra un resumen de los objetivos de la Auditoría Informática.

Fig. 1.4 **OBJETIVOS DE LA AUDITORÍA INFORMÁTICA**



FUENTE: Texto anterior
REALIZADO POR: Investigador

1.7.2 **IMPORTANCIA DE LA AUDITORÍA INFORMÁTICA**

Depende de la visión preventora de los directivos el éxito de la organización y que mejor manera de subsanar o prevenir errores en el funcionamiento del sector informático que la de ejecutar una Auditoría Informática puesto que su naturaleza especializada abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.

Entonces constituye un punto importantísimo dentro de la vida empresarial el vigilar el buen funcionamiento de la misma, de este modo es posible evitar desafortunados desastres que converjan en la pérdida importante de capitales invertidos, así como la destrucción total o parcial de la imagen corporativa causando así estragos negativos en el desempeño de la empresa.

De ahí la importancia de examinar periódicamente el funcionamiento del entorno empresarial con el objetivo de eliminar debilidades y alimentar las fortalezas que tiene toda la entidad o la sección auditada. Es posible apuntar miles de razones importantes para realizar Auditoría Informática en una institución, pero entre las principales tenemos:

- Los fraudes, espionaje, delincuencia y terrorismo informático, son consecuencia de la poca o nula seguridad en los sistemas informáticos instalados en las computadoras, servidores y Centros de Procesamiento de Datos que se han convertido en blancos apetecibles para la delincuencia informática.
- El diseño de las comunicaciones son la base para la continuidad de las operaciones, la administración y organización de la empresa por lo que un sistema deficiente o mal diseñado podría ser un potencial peligro para la empresa.

- La correcta utilización de seguridades y claves de acceso pueden salvaguardar la integridad de las bases de datos que están propensas a atentados y accesos de usuarios no autorizados o intrusos.
- Al no evaluar periódicamente el funcionamiento del departamento informático o no dar soporte técnico adecuado, influyen en la mala imagen e insatisfacción de los usuarios.
- Evaluación de nivel de riesgos en lo que respecta a seguridad lógica, seguridad física y confidencialidad.
- Mantener la continuidad del servicio y la elaboración y actualización de los planes de contingencia para lograr este objetivo.
- El uso inadecuado de la computadora para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor y el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

Todas las razones que se emitieron anteriormente son el justificativo perfecto para la preocupación de directivos y personal informático, además son los indicadores exactos para motivar a la ejecución de Auditoría Informática.

1.7.3 NECESIDAD DE AUDITAR

Al requerir realizar auditoría informática, es innegable la presencia de algunos indicadores en algunos casos muy sutiles y en otros muy claros, por lo tanto el

dirigente de una entidad está en la obligación de tomar atención a las señales que se están haciendo presentes en su empresa.

Cuando se presentan algunos síntomas en las empresas es indiscutible que algo está funcionando mal; entonces, es hora de tomar cartas en el asunto y verificar qué fallas está causando malestar en la institución.

Cuando un sector de la entidad falla es posible observar despejados síntomas que sugieren de necesidad de una Auditoría Informática, señales como:

Descoordinación y desorganización, mala imagen e insatisfacción de los usuarios, debilidades económicas, financieras, inseguridad, etc.

La presencia de uno o todos estos síntomas son avisos claros del mal estar que está siendo presa la empresa, y de la necesidad inmediata de remediar tal situación pero no sin antes evaluar y analizar las posibles causas mediante la aplicación de Auditoría Informática para poder dar soluciones acertadas.

Cuando una institución funciona adecuadamente, todos los procesos y actividades se realizan como engranajes que marcan un solo compás, caso contrario ocurre en el momento en que uno o varios segmentos empiezan a mostrar descoordinación, entonces es hora de revisar cómo se están llevando las tareas.

1.7.4 ALCANCE DE LA AUDITORÍA INFORMÁTICA

El alcance de la Auditoría Informática no es más que la definición del entorno y los límites en que va a desarrollarse la misma; en el informe final, se detalla claramente los temas que fueron examinados, y se indican cuales fueron omitidos.

El ámbito de acción de la Auditoría Informática se puntualiza, en revisar y evaluar, organización de salas de trabajo; compatibilidad de hardware y software; capacitación del personal para la buena atención al cliente; aprovechamiento de las tecnologías; sus controles específicos, los riesgos inherentes a la tecnología, como la seguridad de sus recursos, redes, aplicaciones, comunicaciones, instalaciones y otras.

El alcance que abarca la Auditoría Informática ha de definir con precisión y claridad absoluta el entorno y los límites en que va a desarrollarse.

Estas aclaraciones de la delimitación del área de trabajo se apuntan expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas sea por motivos de seguridad extrema o respeto a las políticas de la institución.

Al realizar auditoría informática es innegable el hecho que se revisará el código fuente, Bases de Datos y por obvias razones la obtención de copias es totalmente prohibida.

Un ejemplo claro de omisión es la inviolabilidad de la integridad de los registros y el control de validación de errores.

Delimitar su ámbito de trabajo, representa una gran ventaja para el auditor de este modo está en la capacidad de organizar de mejor manera el cumplimiento de su investigación.

Con la delimitación del campo de trabajo evita muchos problemas de mal entendidos por omisión de ciertas áreas no auditadas.

1.8 CLASES DE AUDITORÍA INFORMÁTICA

Dentro de las áreas generales, se establecen las siguientes divisiones de Auditoría Informática: de Explotación, de Sistemas, de Comunicaciones y de Desarrollo de Proyectos. Estas son las Áreas Especificas de la Auditoría Informática más importantes.

- De Explotación u Operación,
- Desarrollo de Proyectos, de Sistemas,

- De Comunicaciones y Redes
- De Seguridad.
- En función del sujeto: interna-externa, pública-privada
- En función del alcance: totales o completos parciales o de alcance limitado
- En función del origen del mandato: obligatorias voluntarias
- En función del objetivo: datos personales calidad, cuentas fiscal seguridad
- Según el sector económico: Industria Servicio, etc.

A continuación se explicará brevemente cada una, deteniéndonos un poco más en: auditoría de sistemas. Para dar una visión más clara.

1.8.1 AUDITORÍA INFORMÁTICA DE PRODUCCIÓN O EXPLOTACIÓN

También se la conoce como de Explotación u Operación, ésta se ocupa de revisar todo lo que se refiere con producir resultados informáticos, listados impresos, ficheros soportados magnéticamente, ordenes automatizadas para lanzar o modificar procesos, etc. Auditar la producción, operación o explotación consiste en revisar las secciones que la componen y sus interrelaciones, las cuales generalmente son: Planificación, Producción y Soporte técnico.

1.8.2 AUDITORÍA INFORMÁTICA DE DESARROLLO DE PROYECTOS

En este tipo de Auditoría, se investiga principalmente, la seguridad de los programas en el sentido de garantizar que lo ejecutado por la máquina sea exactamente lo previsto o lo solicitado por el usuario.

Su función principal es la evaluación del desarrollo, análisis y programación de sistemas, basados en los prerequisites del usuario y del entorno, análisis funcional, diseño, análisis orgánico, debido a que si se observan cuidadosamente todos estos detalles se obtendrán excelentes resultados.

1.8.3 AUDITORÍA INFORMÁTICA DE SISTEMAS

La principal preocupación en este tipo de Auditoría es el perfecto funcionamiento de las técnicas de sistemas pues hoy, la importancia creciente de las comunicaciones, líneas y redes de las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de Sistemas. Esta clase de auditoría evalúa algunos aspectos como los siguientes:

Sistemas Operativos: Ésta se encarga del análisis de las versiones de los Sistemas Operativos, su compatibilidad con otros productos de Software Básico, en primer

lugar se verifica si los Sistemas están actualizados con las últimas versiones del fabricante, investigando las causas de las omisiones si las hubiera.

Software Básico: Por razones económicas y de comprobación es indispensable el conocimiento de la facturación del Software Básico aparte de la propia computadora, así fácilmente se podría comprobar que la computadora podría funcionar sin el producto adquirido por el cliente.

Cuanto el Software es desarrollado por el personal informático de la empresa, el auditor debe tomar muy en cuenta los costes que requiere dicha actividad, por si hubiera alternativas más económicas.

Optimización de los Sistemas y Subsistemas: El auditor está en la obligación de verificar que las acciones de optimización fueron efectivas y no variaron la Operatividad de los Sistemas.

Administración de Base de Datos: Si los auditores de Sistemas observan algunas disfunciones en el diseño de las Bases de Datos generalmente debido a la escasa experiencia en esta actividad, deben poner especial atención en esta parte de la indagación.

1.8.4 AUDITORÍA INFORMÁTICA DE COMUNICACIONES Y REDES:

Las redes nodales, líneas, concentradores, multiplexores, redes locales, etc. son el soporte físico-lógico en el ejercicio auditor, es aquí donde se presentan dificultades técnicas del entorno, pues se analiza situaciones y hechos alejados entre sí.

Al auditar comunicaciones y redes es necesario tener conocimiento de la topología de red, actualizada, ya que la desactualización de esta documentación significaría una grave debilidad. La inexistencia de datos sobre cuantas líneas existen, como son y donde están instaladas, supondría que se bordea la inoperatividad informática. Sin embargo, las debilidades más frecuentes o importantes se encuentran en las disfunciones organizativas pues las continuas exigencias por parte de los Usuarios/Clientes de los sistemas de información, así como, la necesidad de adaptarse a las nuevas tecnologías, llevan a las empresas a constantes cambios en sus instalaciones informáticas.

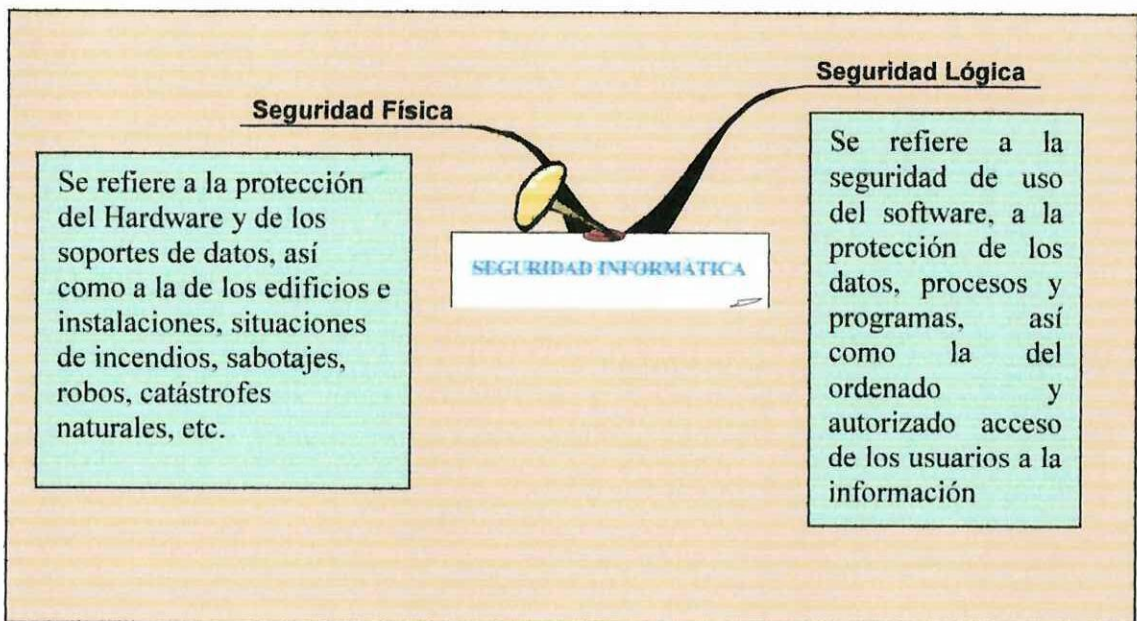
1.8.5 AUDITORÍA DE LA SEGURIDAD INFORMÁTICA

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional.

La Auditoría de seguridad informática abarca los conceptos de seguridad física y lógica. La seguridad física se refiere a la protección del hardware, así como la seguridad de los edificios e instalaciones que los albergan teniendo la visión futurista de posibles incendios, inundaciones, temblores, fallas de energía, catástrofes naturales etc.

En cuanto a seguridad lógica se puede emplear el uso de claves de acceso, integridad de datos, confiabilidad de los mismos, seguridad en el uso de softwares, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información etc.

Fig. 1.5 **SEGURIDAD INFORMATICA**



FUENTE: Texto anterior

REALIZADO POR: Silvana Monge

Un modo eficaz de cuidar nuestra información es tomar en cuenta algunas consideraciones acerca del manejo del equipo disponible, es decir en el uso de disquetes, CDS etc. siendo las principales observancias:

- Verificar contra virus todos los disquetes que se introduzcan en la computadora, aunque sólo sean de datos.
- No ejecutar programas de origen dudoso.
- No meter disquetes extraños.
- Nunca arranque desde disquete en la operación normal de su computadora.
- Nunca dejar puestos disquetes al apagar la computadora.
- Tener la precaución de antes de utilizar disquetes o CD's evaluarlos con un antivirus

1.8.6 AUDITORÍA INFORMÁTICA PARA APLICACIONES EN INTERNET.

El Internet es una red muy extensa en la que se hace muy difícil el control de accesos o la restricción de enlaces, por tanto la auditoria informática pretende evaluar algunos aspectos como los riesgos operativos y tecnológicos, tipos de conexión, etc. como se muestra a continuación:

En este tipo de revisiones, se enfoca principalmente en verificar los siguientes aspectos:

- Evaluación de los riesgos de Internet (operativos, tecnológicos y financieros) y así como su probabilidad de ocurrencia.
- Evaluación de vulnerabilidades y la arquitectura de seguridad implementada.
- Verificar la confidencialidad de las aplicaciones y la publicidad negativa como consecuencia de ataques exitosos por parte de piratas informáticos.
- Evaluar el tipo de conexión con los host
- Examinar los controles de acceso a usuarios.
- Determinar protecciones contra hackers informáticos.
- Evaluar la probabilidad de daños físicos en las conexiones.

1.8.7 AUDITORÍA DE GESTIÓN

En la Auditoría de Gestión se verifica la observancia de normas teóricamente existentes en el departamento de informática y su coherencia con las del resto de la empresa. Para ello, habrán de revisarse sucesivamente y en este orden:

1. Las Normas Generales de la Instalación Informática
2. Los Procedimientos Generales Informáticos. Por ejemplo, la recepción definitiva de las máquinas debería estar firmada por los responsables de Explotación, procedimientos de Backup y recuperación correspondientes.
3. Los Procedimientos Específicos Informáticos. Igualmente, se revisara su existencia en las áreas fundamentales.

1.8.8 AUDITORÍA INTERNA

Dentro de la gran variedad de auditorías, tenemos a la auditoría interna que es aquella realizada con recursos materiales y personas que pertenecen a la empresa auditada. Los empleados que realizan esta tarea son remunerados económicamente.

Cabe aclarar que al tratarse de Auditoría Informática Interna, los auditores deben ser personal extraño al sector informático. La auditoría interna existe por expresa decisión de la Empresa. O sea, que puede optar por su suspensión en cualquier momento, de este modo el auditor interno será un personaje muy alejado del diario quehacer, obteniendo datos confiables y verídicos.

Cuando se ejecuta una auditoría informática interna el auditor debe reunir características especiales, por la familiaridad que tiene con el ambiente de trabajo, por otra parte el éste se encuentra empapado del funcionamiento de su empresa facilitando en gran parte la ejecución de la auditoría informática.

1.8.8.1 VENTAJAS DE LA AUDITORÍA INFORMÁTICA INTERNA

La Auditoría Informática Interna tiene algunas ventajas con respecto a la auditoría externa:

- La auditoría interna tiene la ventaja de que puede actuar determinados periodos de tiempo, Revisando en forma global o parcial los aspectos que quizá presenten fallas.
- Al ejecutar continuamente auditoría, asegura la detección y corrección temprana de errores, a la vez que se convierte en parte del Plan Anual de la empresa.
- Los auditados conocen estos planes y se habitúan a las Auditorías, especialmente si las recomendaciones emanadas afectan positivamente a sus actividades diarias.

1.8.8.2 OBJETIVOS AUDITORÍA INFORMÁTICA INTERNA

Una de las ramas de la Auditoría Informática es la Auditora informática interna que tiene objetivos muy puntuales, los cuales ayudan a la evaluación de la entidad en cuestión.

Entre los principales objetivos que se persiguen en el desarrollo de la Auditoría Informática Interna Tenemos:

- Revisión y evaluación del buen empleo de los recursos informáticos
- Determinación de la utilidad de políticas, planes de contingencia y procedimientos, así como su nivel de cumplimiento
- Custodia y contabilización de archivos, nivel de seguridad de los mismos.

1.8.9 AUDITORÍA INFORMÁTICA EXTERNA

La auditoría externa es aquella ejecutada con recursos materiales y personas que no tengan relación con la empresa auditada, los que deben ser conocedores de informática lo que hace de su investigación un examen totalmente imparcial.

Este tipo de auditoría es requerido por las empresas con el afán de controlar su Informática o puede darse el caso que la institución haya ejecutado una auditoría interna y necesita comparar esos resultados con los de la Auditoría externa, de este modo la entidad cuenta con una segunda opinión que puede determinar si los objetivos del sector informático van de la mano con los de la institución.

1.8.9.1 VENTAJAS DE LA AUDITORÍA INFORMÁTICA EXTERNA

La Auditoría Informática Interna tiene algunas ventajas con respecto a la auditoría externa:

- La Auditoría Externa ofrece la gran ventaja de que el personal empleado en este tipo de examen es totalmente imparcial, por estar ajeno a la actividad empresarial.
- La imparcialidad que se maneja es de vital importancia para emanar un informe final auténtico, sin preferencias ni omisiones.
- Es saludable tener una visión externa del funcionamiento de la empresa.

1.8.9.2 OBJETIVOS DE LA AUDITORÍA INFORMÁTICA EXTERNA

Entre los principales objetivos plantean para la ejecución de la Auditoría Informática Externa tenemos:

- Obtención de elementos de juicio fundamentados en la naturaleza de los hechos examinados
- Medición de la magnitud de un error ya conocido, detección de errores supuestos o confirmación de la ausencia de errores
- Propuesta de sugerencias, en tono constructivo, para ayudar a la gerencia
- Detección de los hechos importantes ocurridos tras el cierre del ejercicio.

Luego de haber dado un enfoque general de los tipos de Auditoría, se puede decir que la Auditoría a ejecutarse es de carácter externo, combinado con la auditoría de gestión, de redes y de seguridad, lo que ayudará a ejecutar una investigación precisa capaz de arrojar los resultados correctos.

1.9 TÉCNICAS DE AUDITORÍA INFORMÁTICA

Las Técnicas Auditoría Informática son métodos prácticos de investigación y prueba para obtener evidencia necesaria que fundamente sus opiniones y conclusiones.

Las técnicas de Auditoría deben ser apropiadas, sencillas, y precisas para evitar operaciones innecesarias, y detalles inútiles. Estas pueden clasificarse de la siguiente forma:

- Técnicas de verificación ocular
- Técnicas de verificación verbal
- Técnicas de verificación escrita
- Técnicas de verificación documental
- Técnicas de verificación física

1.9.1 Técnicas De Verificación Ocular

Son aquellas que le permiten al auditor el conocimiento de algo mediante la apreciación rápida de las circunstancias que ocurren, las técnicas de este tipo son:

- Rastreo exige al auditor seguir la trayectoria de un concepto a fin de determinar la exactitud y precisión d los procesos.
- Comparación es la observación y determinación de la similitud y diferencia de dos cosas, hechos o conceptos, esta técnica permite llegar a conclusiones y recomendaciones.
- Observación es el examen ocular atento a la ejecución de algo, con el objeto de determinar cómo se cumplen las operaciones y cuáles son los procedimientos que se sigue.

- Revisión selectiva es el examen ocular y rápido de los documentos y registros de operaciones realizadas con el fin de separar mentalmente aspectos que no son normales o comunes.

1.9.2 Técnicas De Verificación Verbal

En este grupo se tiene únicamente a la indagación y esta significa la averiguación por información verbal sobre las operaciones y transacciones.

1.9.3 Técnicas De Verificación Escrita

Son aquellas que permiten al auditor el conocimiento de algo como resultado de un trabajo escrito.

Las técnicas que forman parte de este grupo son:

- Análisis significa la obtención de la comprensión de las partes con el fin de obtener un conocimiento sobre el todo
- Conciliación es la determinación de la concordancia entre dos o más cuentas o estados entre sí, originadas por personas diferentes e independientes, pero relacionadas porque se refieren a algo que pertenece a una de ellas.
- Confirmación se busca ratificar que la información proporcionada por la entidad correspondiente a la información entregada por una tercera persona.

La confirmación puede ser:

- Positiva cuando el auditor espera que el destinatario de las solicitudes las conteste, esta puede ser directa o indirecta.
- Positiva directa cuando el auditor entrega la información que desea se le confirme
- Positiva indirecta cuando el auditor no entrega la información que desea confirmar y el destinatario debe recurrir a su propia fuente.
- Negativa cuando el auditor no espera recibir contestación, salvo el caso de inconformidad por parte del destinatario.

1.9.4 Técnicas De Verificación Documental

Son aquellas que le permiten al auditor obtener la seguridad de que las operaciones o transacciones se efectuaron sujetas a las disposiciones internas o externas por medio de los documentos existentes en la entidad.

a) Comprobación.- Es la determinación de que la evidencia documental muestra la naturaleza, propiedad, el importe y la incertidumbre acerca de la operación realizada.

La técnica documental procura:

b) Cálculo.- Mediante el conocimiento de las matemáticas permite la determinación de los valores o cantidades en la verificación de sumas de libros, saldos, etc. dando la seguridad acerca de la exactitud de las cifras.

1.9.5 Técnicas De Verificación Física

Existen prácticas de auditoría que sirven como antecedentes para la aplicación de los procedimientos y el uso de las técnicas de auditoría. Estas prácticas son:

- Las muestras selectivas a juicio del auditor.
- Los síntomas
- La intuición
- La sospecha.

Las muestras selectivas a juicio del auditor. Se basan en el criterio de que el comportamiento individual de los elementos es repetitivo en el universo y que los profesionales de contabilidad y administración son consistentes en sus acciones y criterios por principio.

- b) Por apreciación subjetiva
- c) Muestreo estadístico.

- c) Las muestras por apreciación objetiva pueden ser al azar, periódicas, por bloques, por porcentajes fijos o por porcentajes combinados o conjugados.
- d) El muestreo estadístico aplica técnicas estadísticas para el diseño, selección y evaluación de la muestra.

Los Síntomas.- Son el inicio de algo el echo o acción que se produce como consecuencia de otro.

Intuición.- Es la proyección de los sentidos para la percepción clara e instantánea de un indicio, por lo general es el resultado de un síntoma.

La sospecha.- Es la actitud de recelo o desconfianza que por circunstancias especiales no permite se la otorgue el crédito necesario a laguna información.

La sospecha es el indicador del mal funcionamiento de la empresa, puesto que la información que se tiene difiere de la esperada o se observa la ejecución de procesos fuera de la normalidad.

1.10 METODOLOGÍA DE TRABAJO DE AUDITORÍA INFORMÁTICA

1.10.1 FASE I ESTUDIO PRELIMINAR

En la ejecución de esta fase se copia y revisa documentos que contienen disposiciones 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.

Estudio Preliminar.

- a) Designar Supervisor.
- b) Elaborar notificaciones de inicio de exámenes.
- c) Elaboración del programa de auditoría para esta fase.
- d) Visita a las dependencias del (Área de Procesamiento de Datos) PAD.
- e) Entrevista con los funcionarios.
- f) Obtención de informe general sobre políticas, objetivos, normas, procedimientos “guía de visita previa”.
- g) Análisis de cumplimiento de objetivos establecidos para la creación del PAD.

- h) Elaboración de cédulas analíticas de manuales, instructivos, etc., determinando su aplicabilidad (Normas para código, manual de instructivo de implantación).
- i) Evaluación preliminar de control interno a base de lista de chequeo, o cuestionarios de control interno (visita previa).
- j) Análisis de planes elaborados, grado de cumplimiento, y motivos de su incumplimiento total o parcial.
- k) Informe de cumplimiento de la fase, dirigido al Jefe de Auditoría

1.10.2 FASE II REVISIÓN Y EVALUACIÓN DE RECURSO INFORMÁTICO

En ésta fase se planean y desarrollan cada una de las actividades para las áreas críticas determinadas en la fase II que serán base para el análisis de la fase III.

- a) Elaborar programa de auditoría orientado por la fase II
- b) Ejecutar procedimientos incluidos en el programa de auditoría
- c) Determinar si los errores encontrados son significativos, no significativos o aparentemente significativos.
- d) En caso de encontrar errores no significativos preparar una carta a gerencia con desviaciones.
- e) Elaborar un informe de cumplimiento de la fase II, debiendo aclarar que este no tiene relación con el informe final de Auditoría

1.10.3 FASE III EXAMEN DE ÁREAS CRÍTICAS.

En esta fase mediante planes o programas se investigará con procedimientos a las áreas críticas determinadas en la fase anterior.

Para la organización del trabajo serán necesarios tantos planes como áreas críticas se hayan determinado, de tal manera que se facilite la ejecución por separado; para lograr la identificación de hallazgos en hojas de apuntes.

Para el desarrollo de esta fase se ejecutarán algunos pasos como:

- a) Se procede a elaborar un Plan específico de Auditoría Informática, haciendo constar básicamente los siguientes aspectos:
 1. Motivo de Auditoría.- En el cual se señala la razón por la se originó la auditoría.
 2. Alcance de Auditoría.- Consiste el período que abarca la auditoría, por otra parte se hace constar el ámbito de la auditoría pudiendo ser este toda el área informática, sólo seguridades o sistemas en producción según se delimite la investigación.
 3. Objetivos de Auditoría.- El auditor en este punto precisa los fines o metas que pretende lograr con el examen.

b). Recursos estimados:

Recurso humano.- Se precisa en este punto todas las personas necesarias para la ejecución de Auditoría Informática.

Recurso Financiero.- Se hará constar un estimado del costo y financiamiento del rubro.

Equipos y materiales: Es importante considerar los equipos que van a utilizarse, el Software a emplearse, diskets, CDS, papel continuo, etc.

c). Instrumentos legales.- Se hará constar un listado de disposiciones legales como: políticas internas, normativas y demás documentos que rigen el funcionamiento del área informática.

d). Duración de Auditoría.- Aquí se registrará la fecha de inicio y término de auditoría.

d) Elaborar los planes con los procedimientos para evaluación información de las áreas determinadas como críticas.

e) Cada una de las observaciones y como un documento de apoyo el desarrollo de los procedimientos propuestos en los planes se utilizará hojas de apuntes.

f) Al desarrollar, los planes y consecuentemente los procedimientos se irán encontrando falencias que serán denominadas como hallazgos los cuales serán apuntados en hojas de hallazgos las mismas que constarán del siguiente formato:

1. Título.- En el que se revelará el contenido del hallazgo, éste deberá ser corto y lo más conciso posible.
2. Condición.- Situación encontrada: “Lo que es”
3. Criterio.- Medida, norma, ley aplicable: “Lo que debe ser”.
4. Efecto.- La repercusión de las acciones deficientes, diferencia entre “lo que es y lo que debe ser”.
5. Causa.- los motivos por los que se originó el fallo.
6. Recomendación.- Posible solución para el hallazgo.

NOTA: Cuando se haga referencia a leyes políticas, reglamentos de acuerdo con la necesidad se transcribirá la parte pertinente.

En los hallazgos no constarán nombres de los funcionarios, de ser necesario se hará constar la función que desempeñan.

Se preparará un informe de cumplimiento de la fase mencionando las áreas críticas que se analizaron en los resultados que se obtuvieron y discutir con el Jefe de Auditoría.

1.10.4 FASE IV COMUNICACIÓN DE RESULTADOS.

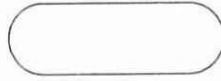
Ésta es la última fase para el desarrollo de Auditoría Informática, es aquí en donde se resume todo el ejercicio auditor plasmado en un informe final.

A continuación se hace referencia a las actividades que se llevarán a cabo en ésta última fase.

- a) Como en las fases anteriores se debe elaborar un plan para el cumplimiento de la fase.
- b) En primer lugar se preparará un esquema del informe en vista que en éste tipo de auditorías no existen modelos definidos de informes como ocurren en las auditorías financieras la estructura del informe final más bien depende del alcance y el ámbito en el examen.
- c) En base a este esquema se elaborará el borrador del informe final de Auditoría, tomando como referencia los hallazgos desarrollados en la fase anterior.
- d) Se convocará a comunicación de resultados a los implicados directos.
- e) Se dará lectura del borrador del informe final de Auditoría.
- f) Como paso siguiente se efectuará los cambios pertinentes y se redactará el informe definitivo de Auditoría Informática.

La simbología utilizada para el flujo diagramación es la siguiente:

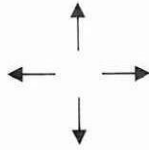
Inicio y fin de proceso



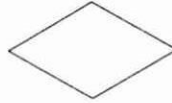
Documento principal



Dirección de flujo



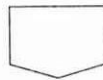
Decisión entre dos alternativas



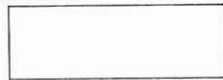
Conector dentro de la página



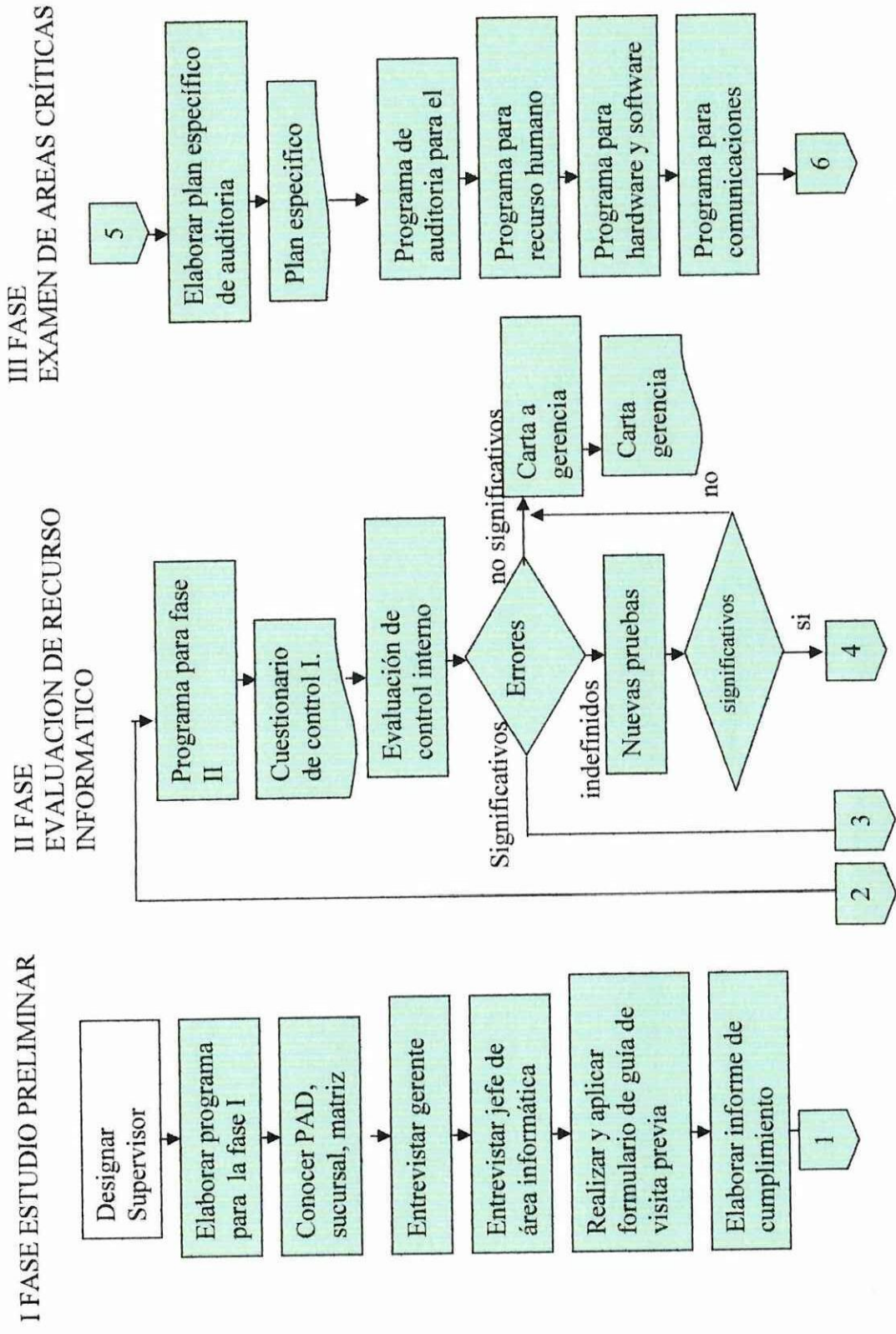
Conector fuera de página

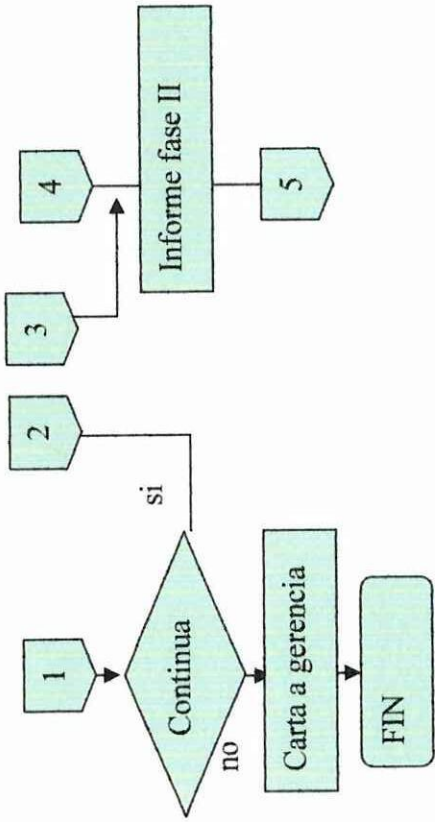
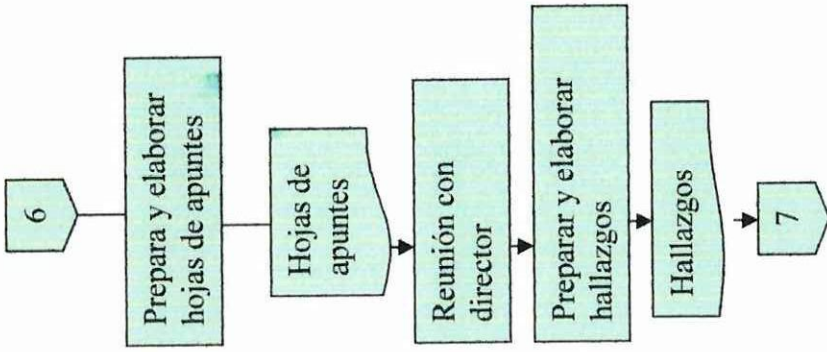


Operación manual

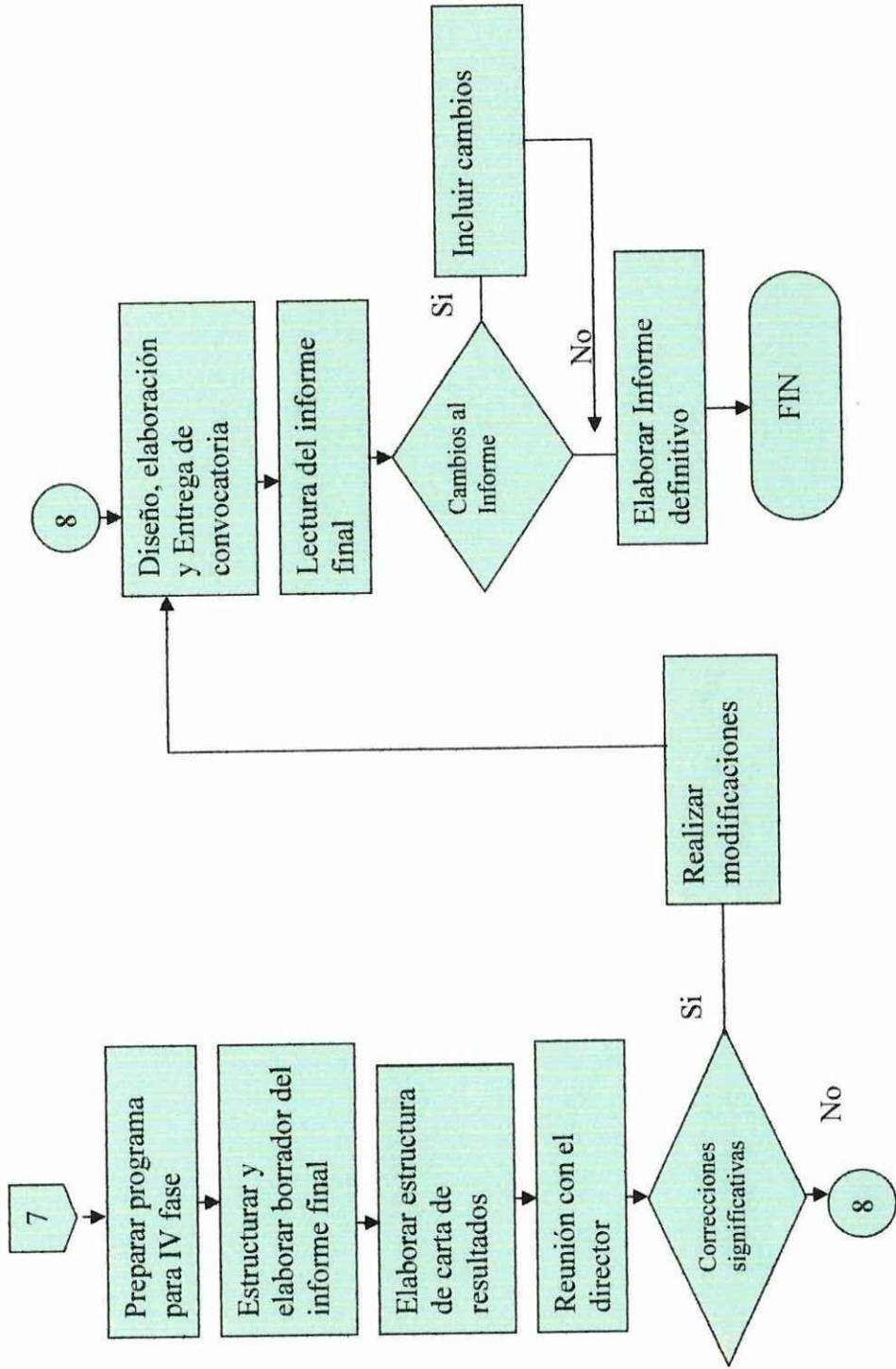


1.12 DIAGRAMA DE FLUJO DE LA METODOLOGÍA PARA RELIZAR AUDITORÍA INFORMÁTICA





IV FASE COMUNICACIÓN DE RESULTADOS



1.13 HERRAMIENTAS PARA EJECUTAR AUDITORÍA INFORMÁTICA

- Cuestionario general inicial.
- Cuestionario Checklist.
- Estándares.
- Monitores.
- Simuladores (Generadores de datos).
- Paquetes de auditoría (Generadores de Programas).
- Matrices de riesgo.

1.14 MODELO CONCEPTUAL DE LA EXPOSICIÓN DEL INFORME FINAL

El informe debe incluir solamente hechos importantes. La inclusión de hechos poco relevantes o accesorios desvía la atención del lector. El Informe debe consolidar los hechos que se describen en el mismo.

El término de "hechos consolidados" adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados.

Hecho encontrado.

- Ha de ser relevante para el auditor y para el cliente.
- Ha de ser exacto, además convincente, y único es decir sin duplicidad.

Consecuencias del hecho

- Las consecuencias deben redactarse de modo que sean directamente deducibles del hecho.

Repercusión del hecho

- Se redactará las influencias directas que el hecho pueda tener sobre otros aspectos informáticos u otros ámbitos de la empresa.

Conclusión del hecho

- No deben redactarse conclusiones más que en los casos en que la exposición haya sido muy extensa o compleja.

Recomendación del auditor informático

- Deberá entenderse por sí sola, por simple lectura.
- Deberá estar suficientemente soportada en el propio texto.
- Deberá ser concreta y exacta en el tiempo, para que pueda ser verificada su implementación.
- La recomendación se redactará de forma que vaya dirigida expresamente a la persona o personas que puedan implementarla.

1.15 CARTA DE INTRODUCCIÓN O PRESENTACIÓN DEL INFORME

FINAL:

La carta de introducción tiene especial importancia porque en ella se resume la auditoría realizada. Se destina exclusivamente al responsable máximo de la empresa, o a la persona concreta que encargó o contrató la auditoría. Así:

- Incluirá fecha, naturaleza, objetivos y alcance.
- Proporcionará una conclusión general, concretando las áreas de gran debilidad.
- Presentará las debilidades en orden de importancia y gravedad.
- En la carta de introducción no se escribirán nunca recomendaciones.

CAPITULO II

ANALISIS E INTERPRETACION
DE RESULTADOS

CAPITULO I I

ANALISIS E INTERPRETACION DE RESULTADOS

2.- LA COMUNIDAD OSCUS

2.1 ORIGEN DE OSCUS

Oscus inició sus labores en España y otros países de Europa, el significado de sus siglas es Organización Social y Cultural Sopeña, DOLORES RODRÍGUEZ SOPEÑA, fue la cabeza fundadora de esta institución, además tuvo la colaboración de distinguidas damas como las Srtas. MARÍA TRUJILLO (+) Y CARMEN LIRIA HARO, uno de los principales colaboradores fue el Obispo de la Diócesis Monseñor BERNARDINO ECHEVERRÍA, y de los Señores: JOSÉ AEERRANO Y ALFREDO PAZMIÑO, todos estos personajes son los mentalistas, y primeros integrantes de Oscus que más tarde crecería hasta conformar una gran sociedad.

El 7 de septiembre de 1966 se dictó la nueva Ley de Cooperativas mediante Decreto Supremo No 1031 y publicado en el Registro Oficial No 123 el 20 de septiembre del mismo año, es así que la Cooperativa procedió a actualizar su estructura y en Asambleas Generales del 5, 12 y 15 de Marzo de 1967 se

aprueban los nuevos estatutos mediante Acuerdo Ejecutivo No 10017 del 12 de Diciembre de 1967 declara la existencia legal de la Cooperativa de Ahorro y Crédito "CENTRO OBRERO DE INSTITUCIÓN" domiciliada en la ciudad de Ambato, por lo que la Dirección Nacional de Cooperativas procede a la reinscripción en el registro correspondiente con el No 197 el 18 de Diciembre de ese año de 1967 Agencias y Sucursales.

Dentro de la comunidad Oscus, tuvo muy buena acogida, los socios cada día se adherían más y más hasta llegar a la necesidad de formar sucursales como es el caso de la Sucursal Latacunga, no siendo esta la única esta gran familia se extiende por varios lugares, especialmente en aquellos donde la corporación requiere de un buen servicio cooperativo.

Por resolución de la Asamblea General de representantes del 11 de abril de 1981, se crea la sucursal de Latacunga, la misma que inicia sus labores el 24 de Octubre del mismo año, correspondiendo el No 200.001 al primer socio señor Gonzalo Fiallo Guevara.

2.2 FUNDAMENTO

La cooperativa OSCUS se fundamenta en el criterio de ser una entidad no lucrativa que proporcionan ventajas económicas a sus asociados, debido a que las cooperativas constituyen a la vez asociaciones de personas y empresas

económicas; y en este último carácter, es innegable que ellas suelen procurar ventajas económicas a sus miembros.

Otro pilar en el que se fundamenta la cooperativa OSCUS es su privacidad, su carácter privado y autónomo reviste a esta entidad cooperativa y hace de ella una de las mejores de la región, presentando la posibilidad del ahorro, obtener buenos servicios pues no sólo es un interés doctrinario sino también interés práctico para poder ayudar a la comunidad, a cumplir con sus sueños, cabe señalar que las cooperativas se manifestaron en el siglo XIX como entidades de carácter privado, de modo que desde sus inicios el movimiento cooperativo ha sabido surgir con sus propios medios.

La ayuda mutua, los préstamos a bajo interés, los cómodos plazos que ofrece la cooperativa OSCUS, son algunos de los beneficios que puede brindar a sus socios, teniendo como fundamento principal la seguridad de los dineros que son depositados en las manos de eficientes empleados que son una parte de la gran comunidad de OSCUS.

2.3 FINES Y MEDIOS

La finalidad principal de Cooperativa de Ahorro y Crédito "OSCUS" Ltda. Sucursal Latacunga es permitir a la comunidad crecer, cumplir sus metas de una manera más rápida y sólida, estas aspiraciones se pueden alcanzar gracias a la

transferencia de capitales desde la cooperativa hacia el prestamista, a cambio se reciben promesas de pago futuro.

Otro fin que persigue la institución, es el de servir de puente para las transacciones que se ejecutan desde fuera del país, debido a las circunstancias que estamos atravesando en la actualidad, con la salida de compatriotas al exterior en busca de días mejores, situación que ha generado la necesidad de enviar dinero a los hogares que se quedan en el país de modo que la cooperativa OSCUS ofrece a sus clientes el servicio de Wester Union, mediante el cual se puede recibir o enviar dinero.

La prontitud y eficacia en el servicio al cliente es una de las mayores preocupaciones de OSCUS; es por ello que se le a puesto especial interés en este punto, y mediante la implementación de cajeros automáticos el cliente puede obtener dinero las 24 horas del día, utilizando la tarjeta VISA ELECTRÓN OSCUS.

El servir eficientemente al socio es la prioridad para OSCUS por lo que trata de actualizar su sistema, sus equipos, dar cursos y charlas a los empleados, etc. todos estos medios son explotados al máximo para dar al cliente el mayor y mejor servicio.

Un fin muy especial que persigue la institución es el de fomentar el ahorro desde tempranas edades, para lo que pone a disposición del cliente menor de 18 años, la oportunidad de guardar dinero en el servicio denominado Mi Tesorito.

Mediante la fomentación del ahorro a tempranas edades, se puede lograr la formación de adultos con visión futurista, uno de los medios de los que hace uso Oscus para crear en los niños y adolescentes el hábito del ahorro.

Todos los fines que persigue, medios que posee OSCUS, son generados, creados, por y para beneficio de toda la comunidad, al tratarse de una entidad no lucrativa, es clara la idea de la búsqueda incesante de días mejores para sus asociados.

La Cooperativa de Ahorro y Crédito Oscus sucursal Latacunga, tiene fines y medios que van en pos de mejorar la calidad de vida de todos sus asociados, poniendo a disposición de los mismos todos los servicios que ofrece Oscus.

2.4 OBJETIVOS, MISIÓN, VISION, FUNCIÓN DE OSCUS

2.4.1 OBJETIVOS DE OSCUS:

- Dar los servicios que requieren los socios para su desarrollo, con el concurso del personal altamente capacitado y equipo de tecnología de punta.

- Estimular el ahorro y el crédito personal, proporcionando las facilidades necesarias, con un interés atractivo.
- Mantener el liderazgo en cuanto a ahorro y crédito se refiere mediante la utilización de tecnología altamente desarrollada además del personal calificado.

2.4.2 MISIÓN DE OSCUS

Quienes conforman la Cooperativa en mención están comprometidos a fomentar el bienestar y el desarrollo socio-económico.

Mejorar el nivel de vida de la comunidad, poniendo a disposición del socio todos los servicios que oscus le ofrece como el ahorro estudiantil, que tiene la misión principal de fomentar en lo más pequeños el ahorro.

2.4.3 VISIÓN DE OSCUS

Al año 2005, lideran el sistema cooperativo brindando excelencia en el servicio y productos financieros a nivel nacional.

2.4.4 FUNCIÓN DE OSCUS

Es saludable fomentar el ahorro entre los componentes de la familia, para incrementar el poder adquisitivo en una forma sencilla. Esta es la verdadera FUNCION SOCIAL de OSCUS.

La permanente práctica de ahorro de nuestros asociados, es la mejor forma de contribuir al fortalecimiento institucional y de conseguir el desarrollo personal y de la familia.

OSCUS es modelo de cooperativismo he ahí otra de sus funciones fomentar el ejemplo para otras instituciones ya que en la ultima revisión de bancos y cooperativas se categorizó a la Cooperativa de Ahorro y Crédito OSCUS Ltda. Sucursal Latacunga como triple A.

Razón por la cual los clientes tienen plena confianza y la total seguridad de que OSCUS sabrá extender la mano para apoyar al pequeño y mediano empresario, artesano o ciudadano común, otorgándole micro créditos a la más baja cuota de interés, por su parte el socio adquiere un compromiso con la institución.

2.5 FUNDADORES Y AUTORIDADES QUE RIGEN OSCUS

OSCUS comienza su trabajo bajo la mirada de su fundadora DOLORES RODRÍGUEZ SOPEÑA, dirigida por las damas Srtas. MARÍA TRUJILLO (+) y CARMEN LIRIA HARO, con apoyo y ayuda del Obispo de la Diócesis Monseñor BERNARDINO ECHEVERRÍA, y de los Señores: JOSÉ AEERRANO Y ALFREDO PAZMIÑO, las siglas de OSCUS significa: “**O**rganización **S**ocial y **C**ultural **S**opeña.

La cooperativa de Ahorro y Crédito OSCUS esta regida por todos sus socios pero cabe aclarar que es necesario una cabeza directriz que guíe el funcionamiento de la cooperativa esta es la Asamblea General de Representantes, la misma que está formada por 41 personas , dicha asamblea es considerada como la máxima autoridad.

El Consejo de Administración está conformado por 5 miembros distribuidos de la siguiente manera: Presidente, Secretario, Primer, Segundo y Tercer Vocal, otro grupo considerado como autoridad de OSCUS es el Consejo de Vigilancia integrado por tres personas: Presidente, Secretario y Vocal, cada una de las personas que forman parte de estos organismos tiene su respectivo suplente en caso de destitución o incapacidad para continuar con las funciones que le han sido delegadas.

La Cooperativa de Ahorro y Crédito OSCUS Ltda. Sucursal Latacunga, está comandada por el gerente, responsabilidad que recae sobre el Ing. Marco Polo Hidalgo, quien ha sabido guiar en forma acertada todas las actividades que en ella se ejecutan.

Mientras existan socios que se beneficien de los servicios OSCUS seguirá existiendo, puesto que sus socios, son la razón de crecer, de ser mejores día con día, la gran familia Oscus, tiene como meta servir a la población que menores recursos económicos posee, debido a la usura que se observa en los bancos, con sus altos intereses.

OSCUS como modelo de ayuda, mutua, solidaridad, y compromiso social es una entidad formada por el pueblo y para el pueblo, en pos de la superación económica de cada uno de los hogares asociados.

2.6 EMPLEADOS DE OSCUS Y SU ROL DENTRO DE LA INSTITUCIÓN

La Cooperativa OSCUS sucursal Latacunga esta conformada por nueve excelentes empleados, estos empleados son administrativos, autoridades, de seguridad, de mensajería, distribuidos de la siguiente manera:

- Gerente
- Secretaria
- Cajera principal
- Cajera secundaria
- Notificador verificador
- Analista de crédito
- Guardia
- Mensajero
- Contador

El rol que cumplen dentro de la cooperativa los empleados es fundamental, de ellos depende la satisfacción del cliente, de su preparación, de la capacidad de relacionarse con el asociado, son la imagen de la cooperativa y con seguridad el socio recibirá la mejor atención, sus requerimientos se cumplirán en el menor tiempo posible debido al alto grado de preparación de cada uno de los integrantes de la familia OSCUS.

Desde el cargo de menor jerarquía hasta el más alto, saben desempeñar con eficacia sus funciones de este modo OSCUS es líder en el movimiento cooperativo, poniéndose a la cabeza de las demás instituciones como modelo financiero. En cuanto a los empleados de OSCUS ocupan los siguientes cargos:

ANALISTA DE CRÉDITOS:	Sr. Luis Chimbo.
NOTIFICADOR VERIFICADOR:	Sr. Raúl Gallegos.
CONTADORA:	Sra. Carmen Moya
SECRETARIA:	Srta. Mariana Silva
CAJERO 1:	Sr. Jonny Herrera
CAJERA 2:	Srta. Sandra Rubio
MENSAJERO:	Sr. Milton Yugsi
GUARDIA:	Sr. William Estrella

El Consejo Administrativo de OSCUS sucursal Latacunga está conformado por:
El Ing. Freddy Morales, Sra. Mónica López, Sr. Vicente Arequipa, y la Sra.
Rosario León.

2.7 SOCIOS DE OSCUS Y SU ROL

La gran familia OSCUS esta formada por 7.500 socios, llenos de sueños y ambiciones que se hacen realidad con la posibilidad del préstamo ya sea este quirografario, emergente, o hipotecario; de dichos préstamos surge el rol del socio de OSCUS

Los socios deben cumplir con sus pagos en las fechas acordadas, la cooperativa confió en el socio, entonces está en la obligación de cumplirle a la cooperativa y

no solo a ella sino al resto de sus compañeros asociados, haciendo honor al fundamento de la institución: ayuda mutua y solidaria.

Los socios de Oscus son la base de la institución, es por quienes la institución funciona, la entidad ha sido creada por los socios y para los socios, el cliente recibe beneficios pero también debe cumplir con obligaciones.

El rol del socio de OSCUS es la cooperación, para la superación personal, familiar y en sí de la comunidad, cuando un socio accede a un préstamo, adquiere un compromiso con la institución

2.8 INFRAESTRUCTURA DE OSCUS SUCURSAL LATACUNGA

La Cooperativa de Ahorro y Crédito sucursal Latacunga cuenta con un edificio de su propiedad ubicado en las calles General Maldonado y Quito.

El local destinado para el funcionamiento de la sucursal Latacunga tiene planta baja y alta con un área de construcción aproximada de 200 m² (10 x 20) en la planta baja se encuentran distribuidas las oficinas de: Gerencia, Secretaria y dos cajas, en la planta alta están ubicadas las oficinas de: Análisis de Crédito y Cobranzas, Contabilidad y Archivo. En la parte posterior de la Institución están ubicadas aulas para cursos de cooperativismo y capacitación del personal.

2.9 PRESENTACIÓN, ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

2.9.1 ENCUESTAS A LOS USUARIOS DEL SISTEMA

CUADRO No 1

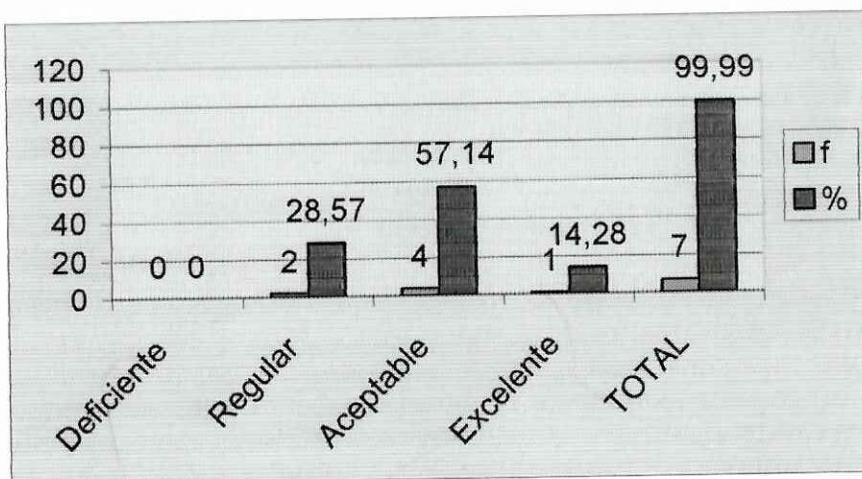
1.- ¿El sistema que está implementado en su institución cubre sus necesidades en forma?:

TABLA # 1 NECESIDADES DEL USUARIO

TITULO: Necesidades del usuario		f	%
1	Deficiente	0	0%
2	Regular	2	28.57%
3	Aceptable	4	57.14%
4	Excelente	1	14.28 %
TOTAL		7	99.99%

FUENTE: Usuarios del sistema encuestados
ELABORACIÓN: Silvana Monge

Fig. 2.1: NECESIDADES DEL EMPLEADO, CON RESPECTO AL SISTEMA



FUENTE: Usuarios del sistema encuestados
ELABORACIÓN: Silvana Monge

En la encuesta aplicada a los usuarios del sistema de la Cooperativa de Ahorro y Crédito Oscus Ltda. Sucursal Latacunga, fue posible recolectar información valiosa es así que a la pregunta numero uno en la que se interrogó sobre la forma en que el sistema cubre las necesidades del usuario del total de encuestados el 57.14% considera que el Sistema Informático usado en Oscus cubre sus necesidades de forma aceptable, en tanto que el 28.57% manifiesta que el sistema cubre sus necesidades de forma regular, este porcentaje corresponde a dos personas.

Los empleados de oscus y usuarios del sistema representados en un 14.28% considera que el sistema cubre sus necesidades laborales de forma excelente, considerando que el 0% corresponde a deficiente.

En condiciones generales, los rangos de aceptación por parte del usuario final se encuentran dentro de la normalidad, puesto que el porcentaje hacia la opción deficiente es sumamente bajo, en caso contrario los resultados arrojados serían altamente preocupantes; debido a que ningún empleado estaría satisfecho con el sistema que utiliza.

De las 7 personas usuarias del sistema en la Cooperativa de Ahorro y Crédito Oscus Ltda. Sucursal Latacunga tan solo 2 personas muestran cierto grado de insatisfacción, cantidad que no es preocupante.

Las tablas y grafica muestran aceptación de los usuarios hacia el sistema.

CUADRO No 2

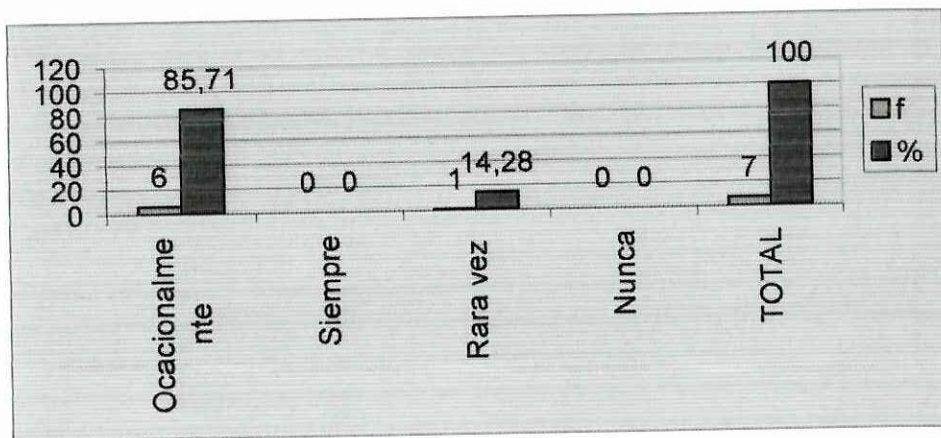
2.- Existen caídas del sistema:

TABLA # 2 CAÍDAS DEL SISTEMA

Caídas del sistema		f	%
1	Ocasionalmente	6	85.71%
2	Siempre	0	0 %
3	Rara vez	1	14.28%
4	Nunca	0	0 %
TOTAL		7	99.99%

FUENTE: Usuarios del sistema encuestados
ELABORACIÓN: Silvana Monge

Fig. 2.2: CAÍDAS DEL SISTEMA.



FUENTE: Usuarios del sistema encuestados
ELABORACIÓN: Silvana Monge

De todos los encuestados el 85.71 manifiesta que ocasionalmente existen caídas del sistema, es decir 6 personas de las 7 encuestadas se ven representadas por este porcentaje, de los mencionados datos se deduce que las caídas del sistema ocurren con muy poca frecuencia, lo que no representa una amenaza o un grave problema para la institución, estos resultados fueron verificados directamente con la observación con la observación de campo por parte del investigador. Estos

resultados nos ayudan a sustentar la teoría de que un sistema bien diseñado, desarrollado e implementado rara o nula vez presenta dificultades en la ejecución del mismo.

Las cifras y porcentajes mostrados en las tablas y graficas son datos verídicos que levantan a la determinación que los usuarios del sistema observan que el sistema es estable es decir que en muy pocas ocasiones este se cae.

El porcentaje es elocuente es decir que nos da a entender que el sistema se encuentra bajo buenos lineamientos para que su funcionamiento sea el mejor posible y esto se ve reflejado en el criterio de los empleados cuando manifiestan la operatividad del sistema.

CUADRO No 3

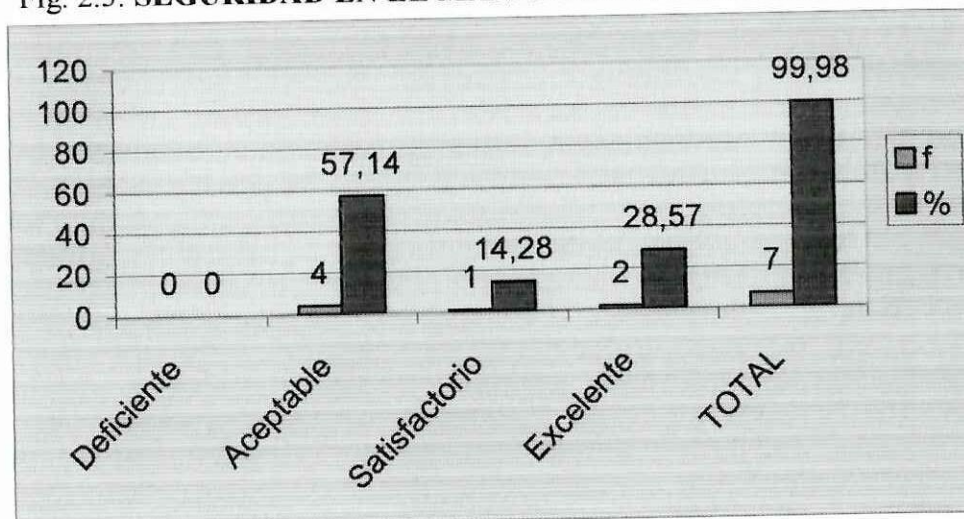
3.- ¿La seguridad establecida en el sistema es?

TABLA # 3 SEGURIDAD EN EL MANEJO DE LA INFORMACIÓN

TITULO: Seguridad en el manejo de la información		f	%
1	Deficiente	0	0 %
2	Aceptable	4	57.14%
3	Satisfactorio	1	14.28%
4	Excelente	2	28.57%
TOTAL		7	99.98%

FUENTE: Usuarios del sistema encuestados
 ELABORACIÓN: Silvana Monge

Fig. 2.3: SEGURIDAD EN EL MANEJO DE LA INFORMACIÓN.



FUENTE: Usuarios del sistema encuestados
 ELABORACIÓN: Silvana Monge

En la encuesta realizada a los usuarios del sistema en la pregunta numero 3 del cuestionario presentado. Que hacia referencia a la seguridad en el manejo de la información, del total de encuestados el 57.14% considera que la seguridad en el manejo de la información es aceptable este porcentaje corresponde a 4 personas.

En tanto que 2 personas están representadas por el 28.57% para satisfactorio, mostrando aceptación por la seguridad empleada en el sistema.

Por otra parte en la opción deficiente el 0% mostrado la tabla y gráfica, corresponde a deficiente; es decir que ninguno de los encuestados opina que la seguridad implementada en el sistema para protección de los datos es deficiente, este es un buen indicador para determinar que el sistema está utilizando seguridades lógicas para proteger los datos de los socios y las cuentas.

Al 14.28% de los encuestados le satisface la seguridad que brinda el sistema en el manejo de los datos.

De estos porcentajes podemos darnos cuenta que el sistema implementado en Oscus cuenta con medidas de seguridad para los datos.

CUADRO No 4

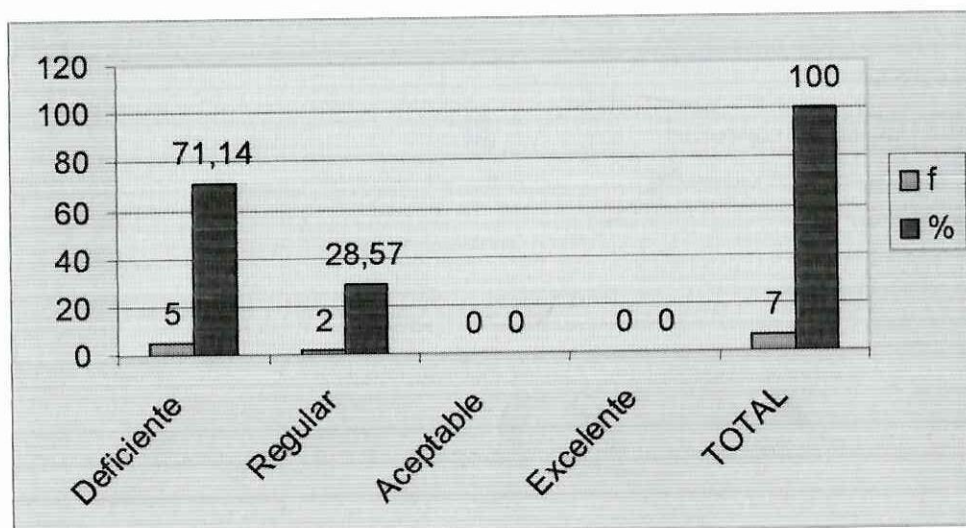
4.- ¿La capacitación o asesoría informática brindada en su institución la considera?

TABLA # 4 ASESORÍA Y CAPACITACIÓN INFORMÁTICA

TITULO: Asesoría y capacitación informática		f	%
1	Deficiente	5	71.42%
2	Regular	2	28.57%
3	Aceptable	0	0%
4	Excelente	0	0%
TOTAL		7	100%

FUENTE: Usuarios del sistema encuestados
ELABORACIÓN: Silvana Monge

Fig. 2.4: ASESORÍA Y CAPACITACIÓN INFORMÁTICA.



FUENTE: Usuarios del sistema encuestados
ELABORACIÓN: Silvana Monge

En la interrogante número 4 se indagó a los encuestados acerca de la capacitación informática que recibe, para determinar su satisfacción o insatisfacción con

respecto al entrenamiento informático que recibe, es así que el 28.57 considera que la capacitación informática impartida en OSCUS es regular.

En tanto que el 71.14%, considera que dicho entrenamiento es deficiente porcentaje preocupante puesto que muestra la insatisfacción del empleado ante la necesidad de obtener conocimientos informáticos.

Los porcentajes mostrados en la tabla y grafica determinan la insatisfacción por parte de los empleados en el entrenamiento de informático.

El porcentaje que se inclina a la opción de deficiente es alto sobrepasando el 50% de los encuestados, indicador que nos lleva a pensar que los operadores del sistema es decir que aquellos que se encuentran en contacto directo con los computadores carecen de buenas bases informáticas.

CUADRO No 5

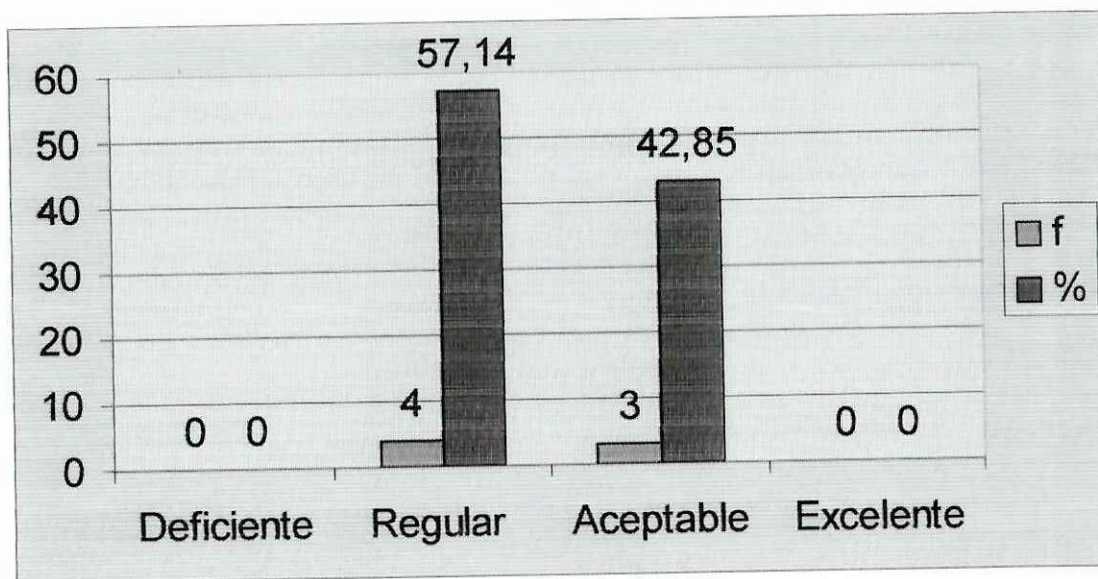
5.- Considera que la red implementada en su institución funciona:

TABLA # 5 FUNCIONAMIENTO DE LA RED

TITULO: Funcionamiento de la red		f	%
1	Deficiente	0	0 %
2	Regular	4	57.14 %
3	Aceptable	3	42.85%
4	Excelente	0	57.14%
TOTAL		7	99.99%

FUENTE: Usuarios del sistema encuestados
 ELABORACIÓN: Silvana Monge

Fig. 2.5: FUNCIONAMIENTO DE LA RED.



FUENTE: Usuarios del sistema encuestados
 ELABORACIÓN: Silvana Monge

En la encuesta aplicada específicamente en la pregunta numero 5 en la que se interrogo a los usuarios del sistema acerca del funcionamiento de la red, para conocer el criterio del usuario ante la ejecución de en la red; de las 7 personas

encuestadas y a la vez usuarias de la red, 4 están representadas por el 57.14%, opinando que el funcionamiento de la es regular, así mismo del total de encuestados 3 opinan que aceptable dando un 42.85%.

Porcentajes que muestra cierta insatisfacción por parte de los usuarios hacia el funcionamiento de la red implementada en la sucursal.

Los usuarios del sistema son los principales evaluadores, es decir que aún sin conocimientos informáticos el usuario está en la plena capacidad de determinar la eficiencia de la red puesto que de los resultados que obtiene al utilizar la misma va generando grados de satisfacción e insatisfacción.

En el caso de esta interrogante en la opción deficiente el 0%, marca la pauta para determinar que el usuario siente que sus necesidades en la red son cubiertas, no de una manera excelente como lo muestra el porcentaje en la opción excelente, pero si de forma regular.

CUADRO No 6

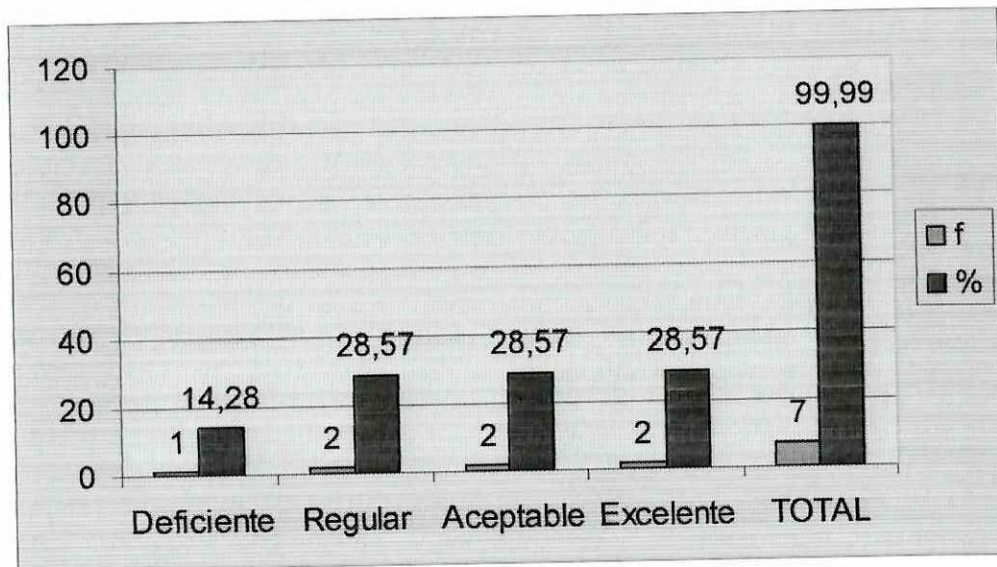
6.- El Hardware y Software que utiliza lo considera:

TABLA # 6 OPINIÓN SOBRE EL HARDWARE Y SOFTWARE

TITULO: Opinión sobre el Hardware y Software		f	%
1	Deficiente	1	14.28%
2	Regular	2	28.57%
3	Aceptable	2	28.57%
4	Excelente	2	28.57%
TOTAL		7	99.99%

FUENTE: Usuarios del sistema encuestados
ELABORACIÓN: Silvana Monge

Fig. 2.6: OPINIÓN SOBRE HARDWARE Y SOFTWARE.



FUENTE: Usuarios del sistema encuestados
ELABORACIÓN: Silvana Monge

Al momento de indagar sobre la satisfacción de respuesta en la ejecución de procesos que se obtiene de los equipos, los encuestados manifiestan en un 14.28% que el hardware y software puesto a su disposición es deficiente.

Así mismo el resto de encuestados se divide equitativamente para el resto de opciones siendo estas regular, aceptable y excelente, con 28.57%, es decir que existe una variedad de criterios que emparejan a las opciones.

El hardware y software son instrumentos de trabajo sumamente importantes, puesto que de la excelente ejecución de los procesos en los equipos de computo depende la satisfacción del empleado tanto como del socio, al recibir éste una respuesta inmediata a sus requerimientos.

Los porcentajes mostrados en la tabla y gráfica anterior se deduce que el hardware y software utilizado en la institución está medianamente actualizado.

CUADRO No7

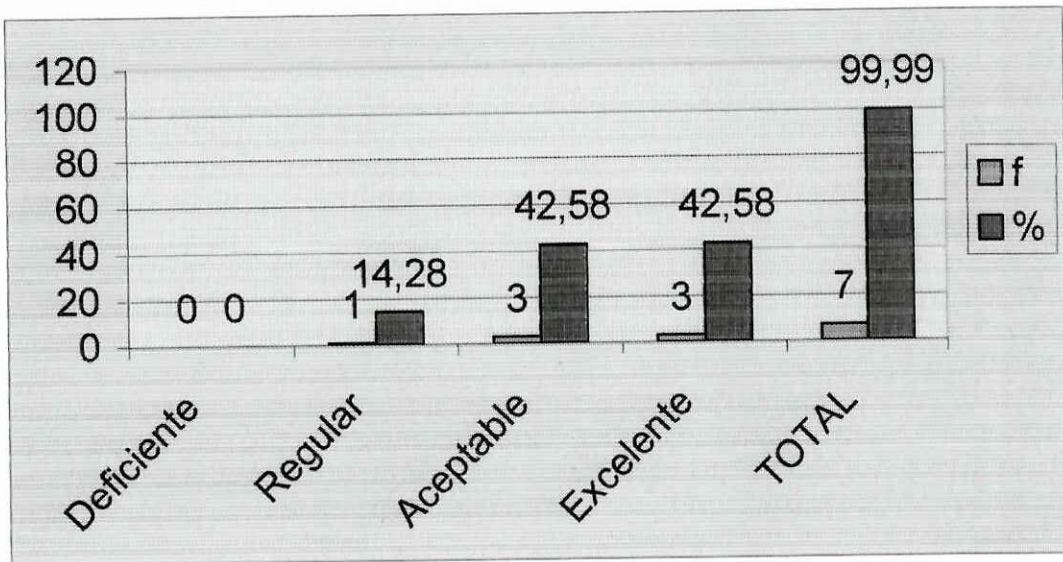
7.- ¿El mantenimiento que le prestan a su equipo lo considera?

TABLA # 7 MANTENIMIENTO DE EQUIPO.

TITULO: Mantenimiento de equipo.		f	%
1	Deficiente	0	0%
2	Regular	1	14.28%
3	Aceptable	3	42.58%
4	Excelente	3	42.85%
TOTAL		7	99.98%

FUENTE: Usuarios del sistema encuestados
ELABORACIÓN: Silvana Monge

Fig. 2.7: MANTENIMIENTO DE EQUIPOS



FUENTE: Usuarios del sistema encuestados
ELABORACIÓN: Silvana Monge

En la pregunta número 7, se indagó a los encuestados sobre el mantenimiento que se le da a los equipos, manifestando el 14.28% que el mantenimiento de los equipos es regular.

Los porcentajes que se muestran entre aceptable y excelente muestran claramente un rango de bienestar en cuanto al mantenimiento que se le da al equipo como al software instalado en los terminales de la sucursal.

Así mismo en la opción deficiente el 0% se hace presente, confirmando la teoría de que el buen mantenimiento de los equipos contribuye al funcionamiento de los mismos pese a que la actualización de estos sea mediana.

Es así que el 42.50% manifiesta que el mantenimiento que se ejecuta en las máquinas de la Cooperativa OSCUS, sucursal Latacunga, es excelente de modo que las máquinas tengan operatividad.

CUADRO No 8

8.- ¿Para mejorar el sistema informático qué le sugiere a la institución?

1.- Que el sistema sea más rápido.

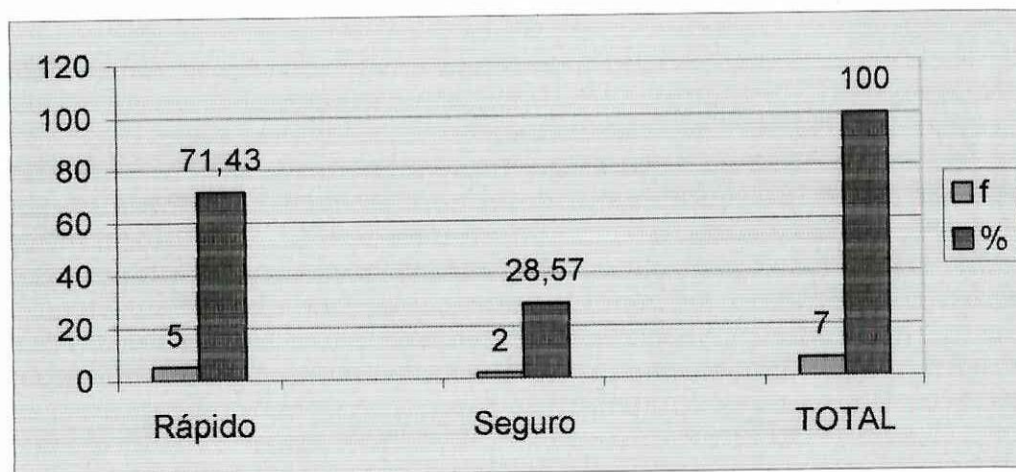
2.- Que se incrementen las medidas de seguridad

TABLA # 8 SUGERENCIAS PARA MEJORAR EL SISTEMA

TITULO: Sugerencias para mejorar el sistema		f	%
1	Rápido	5	71.43%
2	Seguro	2	28.57%
TOTAL		7	100%

FUENTE: Usuarios del sistema encuestados
ELABORACIÓN: Silvana Monge

Fig. 2.8: SUGERENCIA PARA MEJORAR EL SISTEMA



FUENTE: Usuarios del sistema encuestados
ELABORACIÓN: Silvana Monge

El 71% de los encuestados, porcentaje alto, que representa la opinión de 5 personas de las 7 encuestadas, muestran la necesidad de que el sistema sea más rápido en la ejecución de los procesos.

2.9.2 ENCUESTAS A LOS SOCIOS DE OSCUS

CUADRO No 9

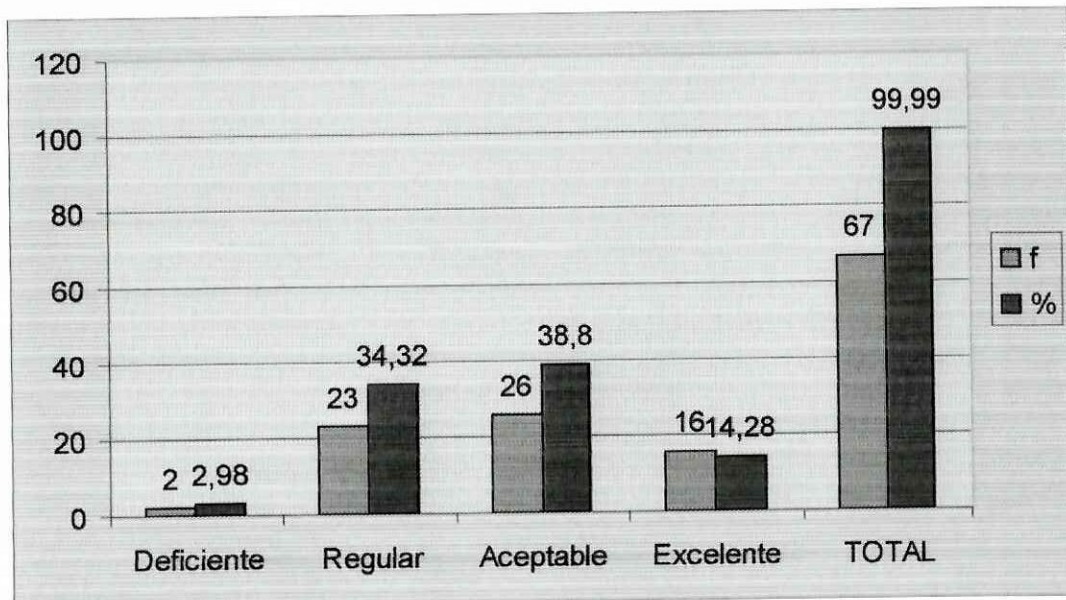
1.- ¿El sistema que se usa en su Cooperativa lo considera?:

TABLA # 9 FUNCIONAMIENTO DEL SISTEMA

TITULO: Funcionamiento del sistema		f	%
4	Deficiente	2	2.98%
5	Regular	23	34.32%
6	Aceptable	26	38.80%
4	Excelente	16	14.28 %
TOTAL		67	99.99%

FUENTE: Usuarios del sistema encuestados
ELABORACIÓN: Silvana Monge

Fig. 2.9: FUNCIONAMIENTO DEL SISTEMA



FUENTE: Usuarios del sistema encuestados
ELABORACIÓN: Silvana Monge

En la encuesta que se realizó a los socios de oscus para determinar el grado de satisfacción hacia el funcionamiento del sistema es así que de los 67 socios

encuestados el 38.80% que corresponde a 26 socios se inclina por la opción aceptable, lo que no lleva a pensar que los socios de Oscus, están satisfechos con el funcionamiento del mismo.

El siguiente porcentaje se encuentra representando a 23 socios con un 34.32% para la opción de aceptable.

El 14.28% de los encuestados manifiestan que el sistema implementado en OSCUS funciona de forma excelente.

De estos porcentajes se deduce que el sistema implementado en OSCUS tiene la aceptación por parte de los clientes o socios.

CUADRO No 10

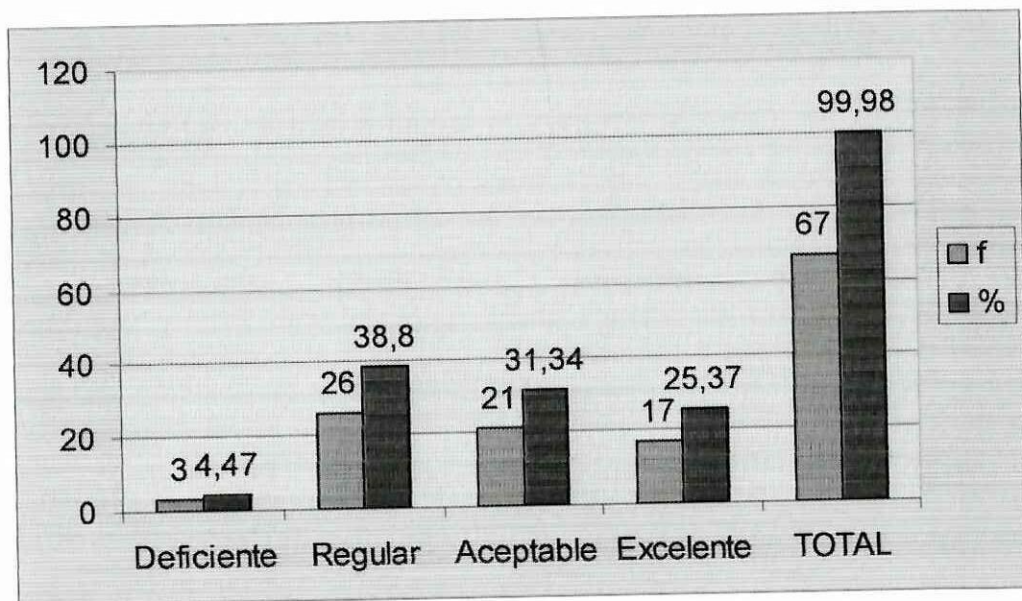
2.- ¿Qué piensa sobre la atención que brindan los empleados de Oscus a sus socios?

TABLA # 10 ATENCIÓN DE LOS EMPLEADOS A LOS SOCIOS

TITULO: Atención de los empleados a los socios		f	%
1	Deficiente	3	4.47%
2	Regular	26	43.28%
3	Aceptable	21	26.86%
4	Excelente	17	25.37%
TOTAL		67	99.98%

FUENTE: Usuarios del sistema encuestados
ELABORACIÓN: Silvana Monge

Fig. 2.10: ATENCIÓN AL CLIENTE



FUENTE: Usuarios del sistema encuestados
ELABORACIÓN: Silvana Monge

Al preguntar sobre la atención que le brinda el empleado al socio, de los encuestados el 43.28% que la atención de los empleados hacia los socios de Oscus es regular.

En tanto que el 26.85% manifiesta que la atención que recibe de los empleados de OSCUS es aceptable.

En este cuestionamiento el 25.37% de los encuestados se inclina por la opción excelente.

De los 67 encuestados 3 socios representados por un 4.47% muestran estar insatisfechos con el funcionamiento del sistema puesto que se inclinan a la opción de deficiente

de lo que se puede deducir que los socios de Oscus muestran cierta insatisfacción hacia la atención que le brindan los empleados de Oscus.

CUADRO No 11

3.- La forma en que desempeñan sus labores los empleados de Oscus la considera:

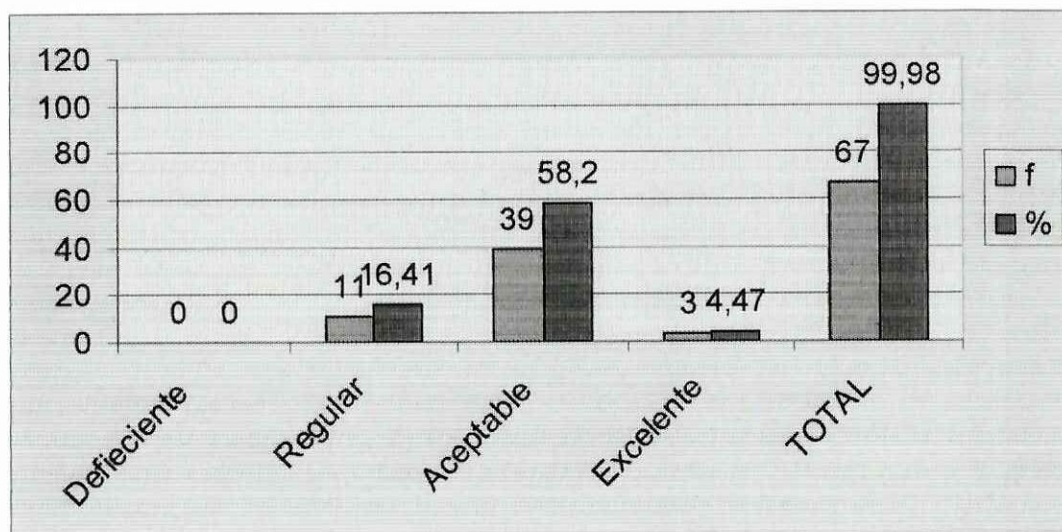
TABLA # 11 LABORES DE LOS EMPLEADOS DE OSCUS

TITULO: Labores de los empleados de Oscus		f	%
1	Deficiente	0	0%
2	Regular	11	16.41%
3	Aceptable	39	58.20%
4	Excelente	3	4.47%
TOTAL		67	99.98%

FUENTE: Usuarios del sistema encuestados

ELABORACIÓN: Silvana Monge

Fig. 2.11: LABORES DE EMPLEADOS EN OSCUS.



FUENTE: Usuarios del sistema encuestados

ELABORACIÓN: Silvana Monge

En la pregunta numero 3 de la encuesta aplicada a los socios de OSCUS en la que se cuestiona sobre el desempeño que tienen los empleados al cumplir con las

labores diarias dentro de la institución el 58.20% considera que los empleados de Oscus desempeñan sus labores de forma aceptable, porcentaje que nos lleva a deducir que los empleados de Oscus se desempeñan adecuadamente al ejecutar las diferentes tareas a ellos designadas.

El 16.41% de los encuestados declara que los socios se desenvuelven en sus labores de forma regular.

El 4.47% cree que los empleados se desempeñan de forma excelente en la ejecución de sus tareas.

Todos estos porcentajes muestran de algún modo la buena imagen que tiene el empleado de oscus ante los socios quienes son los mejores analistas de la situación dentro de OSCUS.

CUADRO No 12

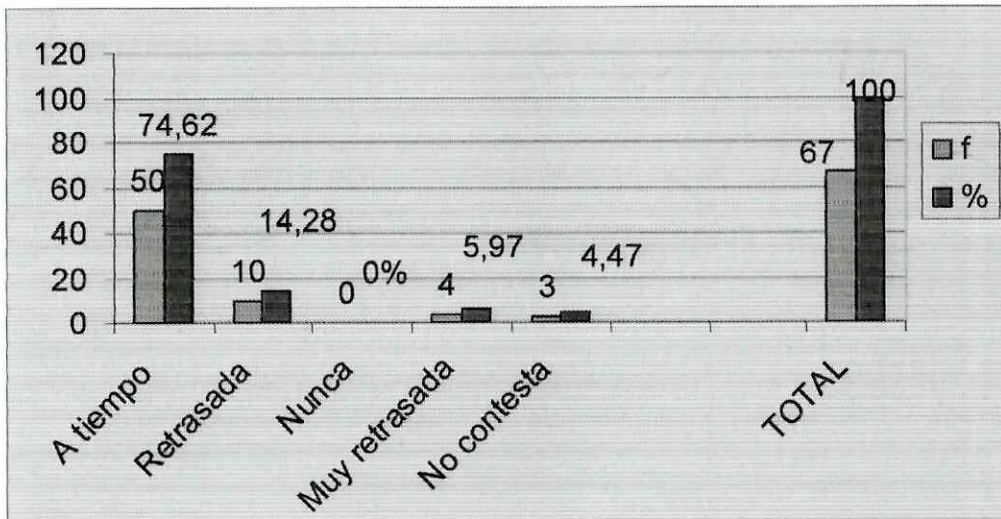
4.- ¿La atención a sus demandas de información como saldos, estados de cuenta, etc. la considera:

TABLA # 12 SERVICIO AL CLIENTE

Respuesta de ciertos requerimientos		f	%
1	A tiempo	50	74.62%
2	Retrasada	10	14.92%
3	No la recibe	0	0%
4	Muy retrasada	4	5.97%
5	No contesta	3	4.47%
TOTAL		67	99.98%

FUENTE: Usuarios del sistema encuestados
ELABORACION: Silvana Monge

Fig. 2.12: SERVICIO AL CLIENTE.



FUENTE: Usuarios del sistema encuestados
ELABORACIÓN: Silvana Monge

El servicio al cliente es un punto importante para determinar si el socio está satisfecho con la ejecución del sistema de modo que al indagar sobre este

cuestionamiento el 74.62% piensa que cuando requiere información la recibe a tiempo.. El 14.92% opina que retrasada.

De estos porcentajes es fácil deducir que la información de cuentas de ahorros, etc. está muy bien organizada.

2.9.3 RESULTADOS DE LAS ENTREVISTAS

Para obtener información real y confiable; se optó por las entrevistas personales a la autoridad competente como es el gerente de la sucursal Latacunga el Ing. Marco Polo Hidalgo Guayaquil, y a los técnicos del Área de Sistemas Informáticos de la Matriz Oscus, en Ambato.

ENTREVISTA AL SR. ING. MARCO HIDALGO GERENTE DE LA SUCURSAL LATACUNGA.

1.- ¿Se han tomado medidas de seguridad en la Sucursal Latacunga?

Se han tomado medidas de seguridad en la institución tales como: alarmas, cámaras de vigilancia que funcionan las 24 horas al día, guardia privado.

2.- ¿Existe una persona responsable de la seguridad?

El responsable de la seguridad, es quien se encarga de contratar la misma, en este caso el jefe de recursos humanos de la matriz, en el caso interno, y externamente el jefe de monitoreo electrónico; de la empresa contratada.

3.- ¿Se contrata vigilancia para la Sucursal Latacunga y se investiga al personal contratado?

No se investiga el personal de vigilancia contratado, puesto que de ello se encargan los empleados pertinentes de la compañía contratada, todas estas circunstancias están estipuladas en las cláusulas del contrato firmado entre la sucursal y la compañía de seguridad denominada

4.- ¿Cuántas horas al día existe vigilancia por parte de un guardia en la Sucursal?

La sucursal se encuentra custodiada por un guardia de vigilancia 12h luego de las cuales se efectúa un relevo.

5.- El edificio está situado a salvo de:

La institución se encuentra situada libre de desastres naturales como inundaciones, fuego, terremotos, de este modo el establecimiento se convierte en lugar seguro tanto para los socios como para los empleados.

6.- ¿ Existe alarma para?

En la Sucursal se ha tomado muy en cuenta el tema de la seguridad tanto física como lógica, por lo que se ha instalado alarmas discriminadoras de audio, detectores magnéticos, de humo, de movimiento, infrarrojos.

7.- Las alarmas están conectadas a:

Las alarmas existentes en la sucursal Latacunga, están conectadas a la Policía Nacional, y las cámaras de vigilancia a la oficina de la matriz de Ocus.

8.- ¿Existen extintores de fuego?

En la sucursal Latacunga existen extintores de fuego, manual, ubicado en sitios estratégicos como en cajas, en la segunda planta cerca al área de créditos se ha ubicado un extintor manual.

9.- ¿Se ha adiestrado al personal en el manejo de extintores en un?

El de Oscus sucursal Latacunga personal esta adiestrado para el manejo de extintores de un 70% a 90%.

10.- ¿Se realizan auditorias periódicas a los medios de almacenamiento masivo?

Ante tal cuestionamiento el Ing. Hidalgo manifestó que no se realizan este tipo de auditorias.

11.- ¿Qué medidas se toman en el caso de extravío de algún dispositivo de almacenamiento?

No se han suscitado casos de esta naturaleza, pero en el caso de ocurrir todo esta controlado por la Matriz.

RESULTADOS DE LA ENTREVISTA AL SR. CARLOS SANTAMARÍA

1.- ¿Quiénes intervienen al diseñar un sistema?

Al diseñar un sistema para la institución intervienen los usuarios, programadores, y un coordinador de sistemas para dirigir a todo el grupo de trabajo.

2.- ¿Los analistas son también programadores, en que porcentaje?

Los analistas del área de sistemas informáticos son también programadores en un 100%, puesto que de ello depende el buen diseño y análisis de los sistemas que se desarrollen razón por demás la creación del sistema implementado en otros.

3.- ¿Qué lenguaje o lenguajes conocen los analistas?

Los analistas conocen lenguajes de programación como: C# Sharp, SQL Server, C, Visual Basic, Java, Oracle, Informix, lo que les da la total capacidad para dar un amplio análisis de cualquier sistema.

4.- ¿Cuántos analistas hay y que experiencia tienen?

Existe un analista y un programador cada quien con tres años de experiencia laboral.

5.- ¿Qué lenguajes conocen los programadores?

Los programadores conocen lenguajes de programación como: C# Sharp, SQL Server, C, Visual Basic, Java, Oracle, Informix, lo que les da la posibilidad de desarrollar un buen sistema.

6.- ¿Cómo se controla el trabajo de los analistas y programadores?

El trabajo del equipo de desarrollo de software se lo controla por tareas, con documentos, y especialmente con la opinión de los usuarios.

7.- ¿Se prueba la corrida de sistemas adquiridos y desarrollados?

Está establecida una etapa de prueba, en el desarrollo de sistemas, previo a la producción.

8.- ¿Se genera pistas y bases para auditoría?

Todo esta documentado, que se tiene una base de datos aplicativa.

RESULTADOS DE LA ENTREVISTA AL SR. JUAN FREIRE

1.- ¿Se restringe el acceso a programas y archivos?

En la entrevista personal realizada al Ing. Juan freire, supo informar que los datos están restringidos.

La seguridad se cuida mediante seguridades como: claves, registros de transacciones, claves y registros en el servidor, además se han tomado muy en cuenta las seguridades físicas.

2.- ¿Los usuarios del sistema pueden modificar los programas y archivos?

Debido a todas las seguridades que se han tomado, los usuarios del sistema no pueden ingresar para modificar el mismo, puesto que existen restricciones de acceso a ciertos módulos del sistema en especial en la parte de programación.

3.- ¿Qué tipo de respaldos usa?

Los respaldos en la cooperativa Oscus se los realiza diariamente en cinta magnética, se obtiene un respaldo antes de fin de día y otro a fin de día.

4.- ¿Con qué periodicidad se hace una revisión física del uso de terminales?

Este tipo de revisión se lo realiza de acuerdo con los requerimientos del usuario, se tiene un grupo externo que da mantenimiento a los terminales.

5.- ¿Se monitorea el uso que se está dando a los terminales?

No, puesto que este tópico no se la ha dado mayor importancia, ni es tan rígido, pero existe un acuerdo de uso de software, la vigilancia del uso de los terminales es un plan a futuro.

6.- ¿Se efectúan auditorías sobre el área de operación y utilización de terminales?

A nivel del sistema no se ha realizado auditoría, pero que en la Cooperativa Oscus se tiene un departamento general de Auditoría.

RESULTADOS DE LA ENTREVISTA AL SR. FRANCISCO LOZADA

1.- ¿Con qué seguridades físicas cuenta la cintoteca?

En el Área de Sistemas Informáticos se cuenta con una bitácora misma que posee seguros, chapas, y además el acceso al área es restringido, solo personal autorizado y previa identificación puede ingresar a este departamento.

2.- ¿Posee un inventario de la cintoteca?

Si existe un inventario, puesto todos y cada uno de los artículos que se encuentran dentro del Área de Sistemas Informáticos debe estar inventariado en forma clara y precisa.

3.- ¿Se registran como parte del inventario las nuevas cintas que recibe la cintoteca?

Todos los materiales que posee el departamento, están claramente especificados en el inventario.

4.- ¿Dónde posee el inventario de la cintoteca?

El inventario se encuentra ubicado en la ciudad de Ambato en la Matriz de Oscus. En este inventario se toma en cuenta datos importantes para llevar el control de las cintas.

5.- ¿Qué información mínima contiene el inventario?

Marca, modelo, número de serie, de los equipos, características y componentes de los servidores.

6.- ¿Qué medio utiliza para almacenar los archivos?

En el Área de Sistemas Informáticos se usa archivos con llave y seguro.

7.- ¿Qué ocurre con los archivos en desuso?

Los archivos en desuso, no se los destruye en el caso de necesitarlos para revisiones posteriores.

8.- ¿Se cuenta con un departamento de auditoría interna para el centro de cómputo?

No existe un departamento de auditoría interna a nivel de toda la institución.

2. 10 VERIFICACION DE HIPOTESIS

Para el desarrollo de la presente investigación se planteó la siguiente hipótesis:

“El desarrollo de Auditoría Informática en la Cooperativa de Ahorro y Crédito Oscus Ltda. Sucursal Latacunga, permitirá un mejor control de los recursos informáticos”

En la Sucursal Oscus Latacunga se aplicaron encuestas a los empleados en su totalidad y a una muestra de sus socios; a los empleados de Oscus se los considera usuarios finales puesto que son quienes diariamente se sirven de dicho sistema para ejecutar sus tareas diaria, razón por la cual se los interrogó con cuestionamientos que al ser respondidos reflejan la opinión que tiene el usuario hacia el servicio informático que está recibiendo, en cuanto a los socios el

principal objetivo fue determinar la satisfacción o insatisfacción que sentía hacia la atención que estaba recibiendo de Oscus.

También se realizaron entrevistas a los integrantes del Área de Sistemas Informáticos, con el objetivo de obtener información sobre el diseño, desarrollo, implementación, mantenimiento, etc. del sistema debido a que son quienes lo crearon, además se realizó entrevista al Sr. Gerente de Sucursal Ing. Marco Hidalgo, para obtener información acerca de la organización, funcionamiento, seguridad, etc. de la Sucursal Latacunga.

Al ser sometido la hipótesis al tratamiento estadístico, mediante la prueba del CHI CADRADO, se niega la hipótesis nula (H_0) y se confirma la hipótesis de investigación (H_1).

Planteamiento de la hipótesis

H_0 : El desarrollo de la Auditoría informática no mejorará el control de los recursos informáticos.

H_1 : La Auditoría informática mejorará los recursos informáticos.

Selección del nivel de significación

Para comprobar la hipótesis utilizaremos un nivel de significación $\alpha = 0,05$

Descripción de la población.

Se extrajeron muestras aleatorias de la población socios de Oscus y se realizaron encuestas a todos los empleados de Oscus sin aplicar fórmula alguna por tratarse de un universo pequeño, a los que se les aplicó un cuestionario:

Especificaciones del estadístico.

Se utilizará la fórmula: $X^2 = \sum [(O - E)^2 / E]$

Especificaciones de las regiones de aceptación y rechazo.

Determinación de los grados de libertad (gl).

Matriz (6x4)

$$gl = (f-1)(c-1)$$

$$= (6-1)(4-1)$$

$$= 5 \times 3$$

$$= 15$$

Según la tabla

Cuando $gl = 15$ y $\alpha = 0,05 \Rightarrow 32,8$

Decisión.

$$X^2_e = 45,84 \geq X^2_t = 32,8$$

Para grado de libertad (gl) = 15 un nivel de significación de 0,05 se obtiene en la tabla 32,8 y como el valor de X^2 45,84 se encuentra fuera de la zona de aceptación de H_0 , se acepta H_1 . Es decir existiría una deficiencia significativa con la auditoría informática en el control de los recursos informáticos.

TABLA No 13: OBTENCIÓN DEL HI CUADRADO

O	E	O - E	(O-E) ²	(O-E)/E
0	0,62	-0,62	0,38	0,62
3	5,91	-2,91	8,47	1,43
0	0,62	-0,62	0,38	0,62
1	0,62	0,38	0,14	0,23
5	0,62	4,38	19,18	30,94
0	0,62	-0,62	0,38	0,62
2	2,54	-0,54	0,29	0,11
26	24,3	1,7	2,89	0,12
4	2,54	1,46	2,13	0,84
2	2,54	-0,54	0,29	0,11
2	2,54	-0,54	0,29	0,11
1	2,54	-1,54	2,37	0,93
4	2,26	1,74	3,03	1,34
21	21,68	-0,68	0,46	0,02
3	2,26	0,74	0,55	0,25
2	2,26	-0,26	0,07	0,03
0	2,26	-2,26	5,11	2,26
3	2,26	0,74	0,55	0,24
1	1,58	-0,58	0,34	0,21
17	15,11	1,98	3,57	0,24
0	1,58	-1,58	2,50	1,58
2	1,58	0,42	0,18	0,11
0	1,58	-1,58	2,50	1,58
3	1,58	1,42	2,02	1,28
				45,84

TABLA No 14 PUNTOS CRITICOS

g.l.	$X^2_{.25}$	$X^2_{.10}$	$X^2_{.05}$	$X^2_{.025}$	$X^2_{.010}$	$X^2_{.005}$	$X^2_{.001}$
1	1.32	2.71	3.84	5.02	6.63	7.8	10.8
2	2.77	4.61	5.99	7.38	9.21	10.6	13.8
3	4.11	6.25	7.81	9.35	11.3	12.8	16.3
4	5.39	7.78	9.49	11.1	13.3	14.9	18.5
5	6.63	9.24	11.1	12.8	15.1	16.7	20.5
6	7.84	10.6	12.6	14.4	16.8	18.5	22.5
7	9.04	12.0	14.1	16.0	18.5	20.3	24.3
8	10.2	13.4	15.5	17.5	20.1	22.0	26.1
9	11.4	14.7	16.9	19.0	21.7	23.6	27.9
10	12.5	16.0	18.3	20.5	23.2	25.2	29.6
11	13.7	17.3	19.7	21.9	24.7	26.8	31.3
12	14.8	18.5	21.0	23.3	26.2	28.3	32.9
13	16.0	19.8	22.4	24.7	27.7	29.8	34.5
14	17.1	21.1	23.7	26.1	29.1	31.3	36.1
15	18.2	22.3	25.0	27.5	30.6	32.8	37.7
16	19.4	23.5	26.3	28.8	32.0	34.3	39.3
17	20.5	24.8	27.6	30.2	33.4	35.7	40.8
18	21.6	26.0	28.9	31.5	34.8	37.2	42.3
19	2.7	27.2	30.1	32.9	36.2	38.6	32.8
20	23.8	28.4	31.4	34.2	37.6	40.0	45.3
21	24.9	29.6	32.7	35.5	38.9	41.4	46.8
22	26.0	30.8	33.9	36.8	40.3	42.8	48.3
23	27.1	32.0	35.2	38.1	41.6	44.2	49.7
24	28.2	33.2	36.4	39.4	42.0	45.6	51.2
25	29.3	34.4	37.7	40.6	43.3	46.9	52.6
26	30.4	35.6	38.9	41.9	45.6	48.3	54.1
27	31.5	36.7	40.1	43.2	47.0	49.6	55.5
28	32.6	37.9	41.3	44.5	48.3	57.0	56.9
29	33.7	39.1	42.6	45.7	49.6	52.3	58.3
30	34.8	40.3	43.8	47.0	50.9	53.7	59.7
40	45.6	51.8	55.8	59.3	63.7	66.8	73.4
50	56.3	63.2	67.5	71.14	76.2	79.5	86.7
60	67.0	74.4	79.1	83.3	88.4	92.0	99.6
70	77.6	85.5	90.5	95.0	100	104	112
80	88.1	96.6	102	107	112	116	125
90	98.6	108	113	118	124	128	137
100	109	118	124	130	136	140	149

Fig. 2.13 PUNTO CRÍTICO DE χ^2

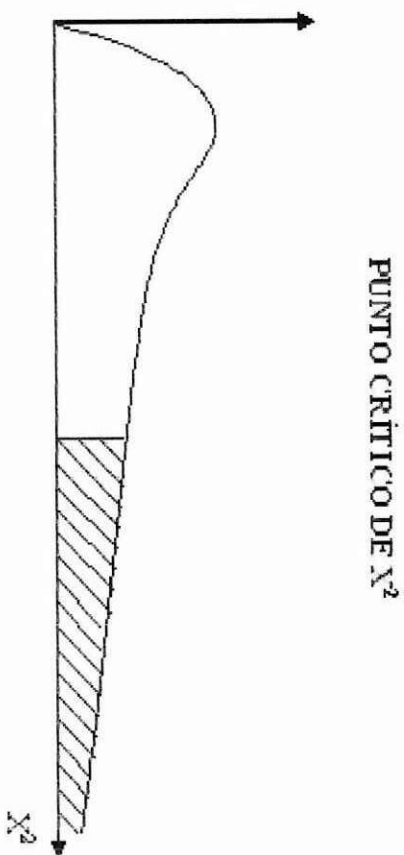


TABLA No 15: TABLA DE FRECUENCIAS

CATEGORIAS	Funcionamiento de la red		Hardware y Software		Accesorios y Capacitación		Mantenimiento		SUBTOTAL DE FRECUENCIA OBSERVADA	SUBTOTAL DE FRECUENCIA ESPERADA
	O	E	O	E	O	E	O	E		
5,91	0	0,62	1	0,62	5	0,62	0	0,62	9	9
24,3	4	2,54	2	2,54	2	2,54	1	2,54	37	37
21,68	3	2,26	2	2,26	0	2,26	3	2,26	33	33
15,11	0	1,58	2	1,58	0	1,58	3	1,58	23	23
7	7	7	7	7	7	7	7	7	102	102

CAPITULO III

PROPUESTA

CAPITULO III

PROPUESTA

3.- EJECUCION DE AUDITORIA INFORMATICA

3.1 TEMA: AUDITORÍA INFORMÁTICA EN LA COOPERATIVA DE AHORRO Y CREDITO OSCUS LTDA. SUCURSAL LATACUNGA

3.2 OBJETIVOS:

- El objetivo principal de desarrollo de Auditoría Informática, es la contribución al mejoramiento del control de los recursos informáticos en la Cooperativa de Ahorro y Crédito OSCUS Ltda.. Sucursal Latacunga.
- Determinar el adecuado uso de los recursos informáticos mediante la aplicación de técnicas y herramientas apropiadas, para obtener resultados consistentes que ayuden al mejoramiento del aprovechamiento de los recursos informáticos que dispone la institución.
- Determinar el estado de la Cooperativa OSCUS a nivel informático, mediante la aplicación de técnicas de auditoria informática, para determinar hallazgos que conlleven a la obtención de conclusiones y recomendaciones acertadas
- Comprobar el funcionamiento del sistema sus aplicaciones, la red establecida, mediante pruebas para observar resultados esperados y obtenidos, para constatar el correcto funcionamiento.

- Verificar la existencia de seguridades para evitar robos y la utilización de copias piratas.

3.3 JUSTIFICACION:

En esta era especialmente en el siglo XX el mundo ha sido testigo de insospechados avances científicos y tecnológicos que en otras épocas le hubiera parecido al hombre producto de la fantasía, una de estas invenciones es el computador, el ser humano en su intelecto ha podido crear máquinas que se convierten en apoyo de las actividades que diariamente desempeña, pero no existe la máquina perfecta, los fantasmas del error se hacen aún más palpables ante el echo de haber sido arrojados por un proceso automático que carece de la exactitud y complejidad del cerebro humano, el computador tiene un margen de error muy reducido pero existente.

Por tal razón quienes emplean computadores para la ejecución de sus tareas deben desechar la idea de que la computadora tiene la razón y empezar a preocuparse por revisar los datos obtenidos, no es la excepción la utilización de sistemas automatizados en entidades o corporaciones financieras como es el caso de la Cooperativa de Ahorro y Crédito "OSCUS" Ltda. Sucursal Latacunga en donde se emplea el computador para manejar grandes cantidades de información, embolsos, desembolsos, transferencia de capitales, apertura, clausura de cuentas de ahorro, apertura seguimiento y clausura de créditos.

También el empleo de una red para ejecutar comunicaciones locales y remotas, que de algún modo puede generar dificultades de manejo, quizá errores, donde se hace necesario revisar cómo esta funcionando la institución, y, que mejor manera que la de realizar una auditoría, en este caso auditoría informática para conocer cómo se están utilizando los recursos informáticos, verificar la satisfacción de los usuarios en cuanto al funcionamiento de la red, las comunicaciones, los sistemas operativos, etc.

El área informática debe ayudar a cumplir con los objetivos de la empresa, reflejar la integridad, el buen manejo de capitales en la superación de los socios de OSCUS.

Con seguridad la auditoría informática es un tema de actualidad porque el mundo gira alrededor de información como: cifras, números, direcciones, etc. que están en constante movimiento, cambian, se incrementan o decrecientan y jamás dejarán de existir, estos datos pueden ser manejados con facilidad gracias al gran invento del computador, instrumento de gran ayuda tanto en casa como en el trabajo, por lo que debe funcionar en optimas condiciones más aún si este funciona conjuntamente con otros ordenadores formando una red de comunicaciones.

Todos los elementos que hacen posible la era de la automatización deben arrojar los resultados esperados, el funcionamiento deseado y en el tiempo estimado, de la evaluación de estos puntos se encarga la auditoría informática, para emitir

criterios que encaminen a la visión futurista de las empresas como es el caso de la Cooperativa OSCUS.

Una de las razones que justifican la aplicación de la auditoría informática es la importancia de tener la información en el momento preciso, en la cooperativa OSCUS es fundamental disponer de datos reales y a tiempo para evitar retrasos que pueden provocar pérdidas considerables.

En la cooperativa OSCUS hasta el momento no se ha realizado una auditoría informática que evalúe el uso de los recursos informáticos, su funcionamiento y estado actual, razón por demás obvia para efectuar una auditoría que arroje resultados imparciales apegados a datos verídicos sujetos a comprobación.

La investigación que se propone evidentemente puede servir como base para futuros trabajos auditores.

Las razones citadas anteriormente, justifican la realización del presente trabajo investigativo, que generará resultados como sugerencias apuntadas en el informe final y de la institución depende acogerlas o desecharlas, en pos de un constante mejoramiento evitando caer en el estancamiento de lo obsoleto e infructuoso.

3.4 FUNDAMENTACION:

las bases legales son un punto muy importante dentro de la investigación, sobretodo al ejecutar Auditoría Informática, es así que la presente se fundamenta

principalmente en las políticas que rigen el control de los recursos informáticos y del área de sistemas; las cuales fueron apuntadas en el primer capítulo.

Como fundamentación de apoyo están las a continuación citadas:

Normas de control para el área de sistemas informáticos.

Normas ISO:2000

Normas del software ISO SPICE.

Normas de documentación de programas ISO 9001

3.5 PRESENTACIÓN:

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

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

Este tipo de organización ayuda al auditor a distribuir de mejor manera su trabajo; como lo dice Montgomery:

El objetivo principal de realizar todo el trabajo en base a planes y programas es organizar todas las actividades evitando de este modo duplicación de tareas, omisión, etc.

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

La información y evidencias son recolectadas aplicando diferentes técnicas de auditoría como se vio en el capítulo anterior; de los resultados de cada una de las tareas ejecutadas depende la determinación de hallazgos, los cuales son base para la obtención de conclusiones y recomendaciones.

La información obtenida en el desarrollo de las actividades es la base para el análisis posterior es así que luego de determinar las tareas cumplidas e incumplidas en los informes en el presente consta un análisis de los datos recolectados, análisis fundamentado principalmente en las políticas de Oscus así como en el reglamento para control de áreas de procesamiento de datos de la Contraloría General del Estado.

En esta fase de la investigación también se presenta la determinación de hallazgos, base fundamental para la redacción del informe final de auditoría, en el cual

contiene los hallazgos encontrados, las causas, efectos, conclusiones y recomendaciones o sugerencias del auditor para mejorar el fallo detectado.

Como se dijo anteriormente la ejecución de tareas esta basada en planes los cuales se presentan a continuación:

3.6 PROGRAMA PARA EL DESARROLLO DE LA FASE I

ESTUDIO PRELIMINAR

Para ejecutar de manera adecuada el estudio preliminar de la Cooperativa de Ahorro y Crédito OSCUS, es necesario establecer un programa de acción como se describe a continuación:

TABLA No 16 PROGRAMA PARA EL DESARROLLO DE LA FASE I

NUM	ACTIVIDAD	ENTIDAD	OBJETIVO	TÉCNICA	INSTRUMENTO
1	Diseño y desarrollo de comunicado de inicio de examen	Sucursal Matriz	<ul style="list-style-type: none"> • Brindar información a los auditados • Obtener predisposición • Evitar inconvenientes 		
1	Visita Previa	Sucursal Latacunga	<ul style="list-style-type: none"> • Identificar el área • Evaluar mediante observación directa. • Obtener información previa. • Observar estado físico de la sucursal 	Guía de visita previa.	Hoja de trabajo
2	Aplicar entrevistas gerente de sucursal Latacunga	Sucursal Latacunga	<ul style="list-style-type: none"> • Obtener información a cerca de la sucursal Latacunga 	Entrevista	Cuestionario
3	Realizar un croquis de la sucursal Latacunga.	Matriz OSCUS	<ul style="list-style-type: none"> • Ubicar geográficamente 	Observación de campo	• Hoja de trabajo

			a Oscus sucursal Latacunga.			
4	Obtener organización funcional y estructural de la sucursal Latacunga.	Sucursal Latacunga.	<ul style="list-style-type: none"> • Determinar jerarquías 	Observación documental	<ul style="list-style-type: none"> • Documentos • Hoja de trabajo 	• Power Point
5	Visita previa	Matriz Oscus	<ul style="list-style-type: none"> • Identificar la institución mediante observación directa. • Obtener información previa. • Observar estado físico de las instalaciones. 	Observación de campo.		
6	Entrevistar al jefe de área informática	Matriz Oscus	<ul style="list-style-type: none"> • Obtener información del funcionamiento del área informática. 	Entrevista	Cuestionario	
7	Realizar un croquis	Matriz Oscus	<ul style="list-style-type: none"> • Determinar ubicación geográfica de la Matriz 	Observación de campo	<ul style="list-style-type: none"> • Hojas de trabajo • Power Point 	de Documento
8	Obtener diagrama funcional y estructural	Matriz Oscus	<ul style="list-style-type: none"> • Determinar jerarquías 	Observación documental		
9	Desarrollar un informe de cumplimiento de actividades.					

Autor: Silvana Monge.

3.7 PROGRAMA PARA EL DESARROLLO DE LA FASE II

EVALUACION DE RECURSO INFORMATICO

TABLA No 17: PROGRAMA PARA EL DESARROLLO DE LA FASE II

NUM	ACTIVIDAD	ENTIDAD	OBJETIVO	TECNICA	INSTRUMENTO
1	Elaborar un cuestionario de control interno	Matriz, sucursal	<ul style="list-style-type: none"> • Obtener información sobre el control de los recursos informáticos 		Hojas de apuntes
2	Aplicación del cuestionario de control interno	Matriz, sucursal	<ul style="list-style-type: none"> • Obtener información 	Entrevista	Cuestionario
3	Evaluación del cuestionario de control interno		<ul style="list-style-type: none"> • Determinar errores 	Observación documental	Cuestionario de control interno
4	Determinar áreas críticas	Matriz	<ul style="list-style-type: none"> • Poseer una orientación para la siguiente fase 	Observación documental	
5	Elaborar carta a gerencia con errores no significativos	Sucursal	<ul style="list-style-type: none"> • Dar a conocer los errores que no representan mayor riesgo para la institución. 		
6	Elaborar un informe de cumplimiento de actividades.		<ul style="list-style-type: none"> • Evaluar el cumplimiento de las actividades propuestas • Resumir en un informe los resultados obtenidos en la fase 		

Autor: Silvana Monge.

3.8 PROGRAMA PARA EL DESARROLLO DE LA FASE III

EXAMEN DE AREAS CRÍTICAS

Una vez determinadas las áreas críticas en la fase anterior, en esta se examinará mediante las siguientes actividades:

TABLA No 18: PROGRAMA PARA EL DESARROLLO DE LA FASE III

NUM	ACTIVIDAD	ENTIDAD	OBJETIVO	TECNICA	INSTRUMENTO
1	Elaboración de un plan específico de auditoría		<ul style="list-style-type: none"> • Organizar correctamente las actividades 		Hojas de apuntes
2	Elaboración de un plan para evaluar el sistema		<ul style="list-style-type: none"> • Obtener información 		
3	Elaboración de un plan de actividades para recurso humano		<ul style="list-style-type: none"> • Determinar errores 	Observación documental	Cuestionario de control interno
4	Elaboración de un plan de hardware y software		<ul style="list-style-type: none"> • Poseer una orientación para la siguiente fase 	Observación documental	
5	Elaboración de un plan de actividades para comunicaciones	Sucursal	<ul style="list-style-type: none"> • Dar a conocer los errores que no representan mayor riesgo para la institución. 		
6	Elaborar un informe de cumplimiento de actividades.		<ul style="list-style-type: none"> • Evaluar el cumplimiento de las actividades propuestas • Resumir en un informe los resultados obtenidos en la fase 		

Autor: Silvana Monge.

TABLA No 19: PLAN PARA LA EVALUACIÓN D EL SISTEMA

La evaluación del sistema que emplea Oscus es un paso muy importante, y mediante la aplicación de técnicas e instrumentos se pretende evaluar el diseño del sistema, estudio de factibilidad, lenguaje de programación, etc. como se muestra a continuación:

PLAN PARA LA EVALUACIÓN D EL SISTEMA					
NUM	ACTIVIDAD	ENTIDAD	OBJETIVO	TECNICA	INSTRUMENTO
1	Elaborar un test		<ul style="list-style-type: none"> • Obtener información sobre análisis, diseño e implementación del sistema 		Hojas de apuntes
2	Aplicación del test al jefe de área	Matriz	<ul style="list-style-type: none"> • Obtener información sobre temas técnicos. 	Entrevista	Test
3	Revisión del estudio de factibilidad del sistema		<ul style="list-style-type: none"> • Evaluar el estudio de factibilidad 	Observación documental	Estudio de factibilidad
4	Solicitar documentación sobre la Base de Datos	Matriz	<ul style="list-style-type: none"> • Examinar tipo, diseño, plataforma, etc. 	Observación documental	
5	Solicitar documentación del código fuente	Matriz	<ul style="list-style-type: none"> • Evaluar el lenguaje de programación, sintaxis de las líneas de código. • Determinar el uso de clases. 	Observación documental	

6	Aplicar encuestas a los empleados	Sucursal	<ul style="list-style-type: none"> • Conocer el criterio de los empleados, sobre el sistema 	Encuesta	Cuestionario
7	Aplicar encuestas a los socios	Sucursal	<ul style="list-style-type: none"> • Conocer el criterio de los socios 	Encuesta	Cuestionario
8	Solicitar manual de usuario	Matriz	<ul style="list-style-type: none"> • Comprobar la existencia, distribución, manejo, del manual de usuario 	Observación documental	Manual de usuario
9	Solicitar plan de contingencias	Matriz	<ul style="list-style-type: none"> • comprobar la existencia de un plan de contingencias del área informática en función del sistema que emplea Oscus 		
9	Obtener reportes generados por el sistema	Sucursal	<ul style="list-style-type: none"> • Observar la información contenida en los reportes 	Observación documental	Reportes
6	Manipular las aplicaciones	Sucursal	<ul style="list-style-type: none"> • Comprobar el funcionamiento de las aplicaciones, control de restricciones, validaciones, mediante datos prueba y reales. 		Sistema Sifz Os
11	Realizar un estudio FODA		<ul style="list-style-type: none"> • Determinar fortalezas, oportunidades, debilidades y amenazas del sistema 		

Autor: Silvana Monge.

TABLA No 20: PLAN PARA EL ANÁLISIS DEL RECURSO HUMANO

PLAN PARA EL ANÁLISIS DEL RECURSO HUMANO						
NUM	ACTIVIDAD	ENTIDAD	OBJETIVO	MÉTODO	INSTRUMENTO	
1	Visita a institución de OSCUS	Sucursal Latacunga	<ul style="list-style-type: none"> • Verificar de No. puestos • Verificar No. empleados • Determinar necesidad del puesto de trabajo 	Obs. directa	Hoja trabajo	
2	Obtener currículos empleados	Sucursal Latacunga	<ul style="list-style-type: none"> • Observar el nivel académico de empleados, experiencia laboral, etc. 	Observación documental	Curriculums	
3	Observar contratos de trabajo	Matriz	<ul style="list-style-type: none"> • Comprobar la legalidad y que se respete derechos empleados con vacaciones, maternidad, etc. 	Observación documental	Hoja trabajo	
4	Obtener copias de los contratos de trabajo	Matriz	<ul style="list-style-type: none"> • Obtener un documento fidedigno que avalice la legalidad del trabajo de los empleados de OSCUS. 	Observación documental	Contratos de trabajo	
5	Realizar un detalle de las funciones de los empleados	Sucursal Latacunga	<ul style="list-style-type: none"> • Comprobar la existencia de jerarquias 			
6	Entrevista Gerente	Sucursal Latacunga	<ul style="list-style-type: none"> • Obtener información desde la fuente autoridad. 		Hoja trabajo	
7	Aplicar encuesta empleados OSCUS	Sucursal Latacunga	<ul style="list-style-type: none"> • Obtener información desde el punto de vista de los empleados. 	Encuesta	Cuestionario	

A. Ibor Si vanni Monge.

TABLA No 21: PLAN PARA EVALUACIÓN DE HARDWARE Y SOFTWARE

PLAN PARA EVALUACIÓN DE HARDWARE Y SOFTWARE					
NUM	ACTIVIDAD	ENTIDAD	OBJETIVO	TÉCNICA	INST
1	Visitar las instalaciones de sucursal	Sucursal Latacunga	<ul style="list-style-type: none"> -Observar el estado físico de los equipos - Observar el estado de la instalación eléctrica y cableado. -Determinar la ubicación de los equipos - Verificar el estado del cableado - Auscultar el estado de equipos de comunicaciones -Observar la seguridad física de los equipos 	Observación directa	Hoja trabajo
2	Diseñar y elaborar un sello adhesivo	Sucursal Latacunga	<ul style="list-style-type: none"> -Constatar la revisión física de los equipos 		<ul style="list-style-type: none"> -Adhesivo -Paint -Power Point -Scanner
3	Diseñar y elaborar un certificado de revisión de equipos	Sucursal Latacunga	<ul style="list-style-type: none"> -Obtener un documento firmado por los encargados de los equipos que avalice la revisión física de los mismos 		Certificado
4	Instalar Software Task Info en máquinas de OSCUS	Sucursal Latacunga	<ul style="list-style-type: none"> -Determinar software instalado -Observar programas activos -Detectar instalaciones y uso de antivirus -Determinar características del cpu 		TASK INFO

				-Observar las comunicaciones entre terminales -Observar SO de c/u de las máquinas -Contrastar el inventario realizado con el proporcionado por OSCUS		Observación directa, Observación documental	Hoja trabajo
5	Realizar un inventario	Sucursal Latacunga					
6	Graficar la ubicación geográfica de equipos	Sucursal Latacunga		-Determinar ubicación de equipo y su funcionalidad		Observación directa	Hoja trabajo
7	Diseñar y elaborar un modelo virtual de las instalaciones de OSCUS	Sucursal Latacunga		-Determinar aprovechamiento espacios seguridad, puertas, acceso, salidas, auxilios, etc.		Observación directa	-Hoja trabajo -Autocad
8	Manipular los equipos	Sucursal Latacunga		-Determinar la operatividad del hardware y software		Observación directa Manipulación	-Equipos de la Sucursal Latacunga -Hoja de trabajo
9	Ejecución de TASK INFO	Sucursal Latacunga		-Obtener información			TASK INFO
10	Repetir proceso anterior			-Comparar resultados			
11	Analizar Información Obtenida con Task Info			-Evaluar software instalado, operatividad, uso, etc.		análisis	

Autor: Silvana Monge.

TABLA No 22: PLAN PARA EVALUACIÓN DE LA RED

PLAN DE ANÁLISIS DE RED					
NUM	ACTIVIDAD	ENTIDAD	OBJETIVO	TÉCNICA	INSTRUMENTO
1	Obtener el diseño de la Red	Matriz	-Evaluar el diseño de la Red	Observación documental	-Software Network diagram
2	Graficar puntos de Red	Sucursal Latacunga	-Evaluar ubicación y funcionalidad de los terminales	-Observación documental -Observación directa	-Hojas de trabajo -AUTOCAD
3	Observar el estado del cableado	Sucursal Latacunga	-Evaluar mantenimiento del cableado	-Observación directa	-Hojas trabajo
4	Monitorar la Red Instalar software.	Matriz	-Evaluar tiempos de transmisión y recepción -Determinar Anchos de banda	Manipulación	-Software -Ethereal - PRTG Traffic Grapher
5	Analizar la información recolectada		-Obtener u resumen de todos los puntos encontrados		

Autor: Silvana Monge.

3.9 PROGRAMA PARA EL DESARROLLO DE LA FASE IV

TABLA No 23: COMUNICACIÓN DE RESULTADOS

PLAN PARA LA EJECUCIÓN DE LA FASE IV				
NUM	ACTIVIDAD	OBJETIVO	TÉCNICA	INSTRUMENTO
1	Preparar extractora del Informe final	-Estructurar el Informe Final	Investigación bibliográfica	-Manual de Auditoría Informática
2	Reunión con asesor	-Corrección de errores		
3	Prepara estructura de convocatorias	-Estructurar Convocatorias	Investigación bibliográfica	-Manual de Auditoría Informática
4	Diseñar y elaborar carta de introducción	-Comunicar resultados	-Observación directa	-Hojas trabajo
5	Elaboración del borrador del Informe final			
6	Entrega de invitaciones			- Microsoft publisher
7	Lectura del Informe Final	-Comunicación de resultados -Corrección de errores		
8	Ejecutar cambios			
9	Elaboración del Informe Final			

Autor: Silvana Monge.

3.10 INFORMES DE CUMPLIMIENTO DE ACTIVIDADES

3.10.1 INFORME DE CUMPLIMIENTO DE ACTIVIDADES DE LA FASE

I



UNIVERSIDAD TECNICA DE COTOPAXI



INFORME DE CUMPLIMIENTO DE FASE I

TEMA TESIS: Auditoria Informática en la Cooperativa de Ahorro y Crédito
Oscus Ltda. Sucursal Latacunga

AUTOR: Silvana Monge

DIRIGENTE: Ing. Emma Campaña

TEMA: Fase Preliminar

OBJETIVOS:

- Comunicar al personal de la cooperativa “Oscus” sucursal Latacunga, el inicio de examen de auditoria, mediante circulares, para el conocimiento de los auditados.
- Aplicar el cuestionario de guía de visita previa.
- Conocer ubicación, distribución de equipos personal, archivos, etc. por medio de las visitas personales a las dependencias para constatación física del estado de las instalaciones.

- Obtener documentación como organigramas estructurales y funcionales, manuales, instructivos, reglamentos, políticas, etc. a través de solicitudes verbales y escritas para observar la existencia, cumplimiento de las normativas que rigen la institución.
- Solicitar planes de actividades como por ejemplo de capacitación, mediante peticiones verbales, para observar el cumplimiento de de la entidad especialmente a nivel informático.

MATERIALES EMPLEADOS:

Para la ejecución de la primera fase denominada preliminar se utilizo lo siguiente:

- Circulares de inicio de examen
- Hojas de trabajo indicado
- Formulario de guía de visita previa
- Solicitudes verbales y escritas para obtener documentación.

DESARROLLO:

Como primer paso y atendiendo al objetivo número uno, se presentaron comunicados de inicio de examen, en el que se hizo constar la fecha de inicio de auditoria así como el período que comprenderá la misma, de este modo todas la personas involucradas en el desarrollo de auditoria, tendrán conocimiento y

predisposición para colaborar en la ejecución del trabajo, Para mejores detalles podemos observar la estructura de dicho comunicado en el anexo número 1. Que se lo presenta en un instrumento de apoyo como lo es un CD de datos.

En segundo lugar se realizaron visitas personales al ambiente de trabajo de Oscus, con el objetivo de familiarizar e identificar el área a ser auditada, en este caso la sucursal Latacunga. Como lo muestra el anexo número 2., presentado en el CD.

Otra tarea cumplida fue la aplicación de un formulario denominado guía de visita previa como lo muestra el anexo numero 9. La siguiente tarea ejecutada es la realización de una entrevista con el gerente de la Sucursal Latacunga que se muestra en el anexo número 4.

Mediante la visita a OSCUS y el trabajo de campo fue posible diseñar y elaborar un croquis de la institución con el objetivo de ubicar geográficamente al edificio donde funciona OSCUS Sucursal Latacunga., como se muestra en el anexo número 3. (Presentado en el CD de apoyo).

Otra tarea cumplida es la obtención del diagrama estructural de la sucursal Latacunga donde se muestra la jerarquía de sus empleados. Como se muestra en el anexo número 5 presentado en el CD.

En el transcurso de la investigación se requerirán datos técnicos que son del conocimiento de los creadores del sistema, por tanto se hizo necesario visitar el área de informática que funciona en la matriz de Oscus.

Además se realizó una entrevista al Ing. Carlos Santamaría jefe de área se obtuvo información acerca de la formación profesional de los analistas, programadores, manifestando que los mismos tienen experiencia de trabajo, buena formación profesional y están en capacidad de desarrollar software es así que forman parte del equipo que diseñó y desarrolló el sistema que emplea Oscus. Como lo muestra el anexo número 6.

Otra tarea cumplida fue el diseño y elaboración de un croquis de la Matriz de Oscus, con el objetivo de determinar la ubicación geográfica del edificio. Como se muestra en el anexo número 7 del CD de apoyo.

De igual manera el área de informática establece su grado de responsabilidad poniendo a la cabeza al jefe de área le sucede el administrador, quien es seguido por el analista, cada uno cumple funciones específicas. Como se muestra en el CD anexo número 8.

3.10.2 INFORME DE CUMPLIMIENTO DE ACTIVIDADES DE LA FASE II



UNIVERSIDAD TECNICA DE COTOPAXI



INFORME DE CUMPLIMIENTO DE FASE II

TEMA TESIS: Auditoria Informática en la Cooperativa de Ahorro y Crédito

Oscus Ltda. Sucursal Latacunga

AUTOR: Silvana Monge

DIRIGENTE: Ing. Emma Campaña

TEMA: Evaluación de recurso informático.

Objetivos:

- Diseñar un cuestionario de control, para obtener información del control de recurso informático.
- Determinar áreas críticas en base a investigaciones del uso de los recursos informáticos.

MATERIALES EMPLEADOS

- Cuestionario de control del uso de recurso informático.
- Hojas de trabajo
- Hoja de apuntes

DESARROLLO

Una vez reconocida el área de trabajo y determinada la necesidad de ejecución de Auditoría Informática en la sucursal Latacunga, se procedió a diseñar para luego aplicar un cuestionario de control interno como lo muestra el anexo número 10, contenido en el CD de anexos, para obtener información sobre algunos tópicos como seguridades, controles físicos, en programas, aplicaciones, mantenimiento de equipos, análisis desarrollo de sistemas, manejo de equipos, etc.

Otra tarea ejecutada fue la determinación de áreas críticas, este punto se realizó tomando en cuenta toda la información obtenida en la fase anterior como los son las entrevistas el cuestionario de guía de visita previa, las entrevistas y por su puesto el cuestionario de control interno.

La siguiente tarea desarrollada fue la determinación de errores, diferenciando los no significativos, para los que se redactó una carta a gerencia en donde se redacta los errores encontrados y las sugerencias de soluciones como lo muestra el anexo número 11. contenido en el CD de apoyo.

3.10.3 INFORME DE CUMPLIMIENTO DE ACTIVIDADES DE LA FASE

III



UNIVERSIDAD TECNICA DE COTOPAXI



INFORME DE CUMPLIMIENTO DE FASE III

TEMA TESIS: Auditoria Informática en la Cooperativa de Ahorro y Crédito

Oscus Ltda. Sucursal Latacunga

AUTOR: Silvana Monge

DIRIGENTE: Ing. Emma Campaña

TEMA: Examen de áreas críticas.

Objetivos:

Para esta fase se han planteado los siguientes objetivos:

- Elaboran un plan específico de auditoría, para organizar de mejor manera las actividades, mediante la planeación estratégica de cada una de las acciones a tomarse.
- Elaborar sendos programas para examinar cada área.
- Preparar y elaborar hojas de hallazgos.
- Elaborar un informe final que resuma todas las actividades cumplidas y los resultados obtenidos.

Como primer paso para el cumplimiento de esta fase es diseñar un plan específico de auditoría, este plan sirve de guía en la ejecución de actividades evitando omisiones, duplicaciones de tareas, etc. esta actividad planteada en el plan de fase III, fue cumplido para mayores detalles dicho documento se encuentra detallado en el anexo número 12, contenido en el CD de anexos.

3.10.3.1 INFORME DE TAREAS CUMPLIDAS DEL PLAN PARA EVALUAR EL SISTEMA

De acuerdo con plan estratégico de fase y plan de recurso sistema, se aplicó un test, al Ing. Carlos Santamaría como consta en el anexo número 13, contenido en el CD de anexos, este documento tiene por objetivo determinar diseño, evaluación e implementación del sistema por parte de sus creadores. Esta actividad se cumplió satisfactoriamente.

Otro paso que se cumplió dentro de lo planificado es la comprobación de un estudio de factibilidad desarrollado antes de la implementación del sistema que se encuentra funcionando actualmente en Ocus.

Dentro de lo programado esta la constatación de documentación de la Base de datos para obtener información sobre la plataforma, tipo, diseño de la Base de Datos, también este paso fue cumplido, así como la obtención de documentación

del código fuente, lamentablemente en esta tarea no se pudo cumplir la obtención de copias de la base datos y código fuente por políticas de seguridad.

También se aplicaron encuestas a los usuarios del sistema con el objetivo de obtener información a cerca de datos importantes como capacitación informática, satisfacción con el sistema, etc. como se puede apreciar en el anexo número 14.

Otro paso importante que se cumplió es un análisis FODA del sistema como se muestra a continuación:

TABLA No 24: ANALISIS FODA

FORTALEZAS	OPORTUNIDADES	DEBILIDADES	AMENAZAS
<ul style="list-style-type: none"> • Cantidad adecuada de equipos. • Compatibilidad de Hardware y Software. • El sistema esta programado en un lenguaje de actualidad como es el C# • Tienen desarrollo propio de software adaptado a sus necesidades. • Poseen muy buena seguridad lógica. • Existe buen desempeño de los empleados en labores generales. 	<ul style="list-style-type: none"> • Si se actualizan los equipos no existirán egresos innecesarios. • Implementar un plan de contingencia adaptado a la Sucursal Latacunga con conocimiento pleno de este por parte de los usuarios del sistema con esto se estará preparado para responder adecuadamente a posibles desastres. • La empresa está sujeta cambios y crecimiento al igual que el sistema. • Flexibilidad en la programación. • Con el presente estudio 	<ul style="list-style-type: none"> • Equipo medianamente actualizado. • Caídas del sistema • Cobertura parcial de las necesidades de los usuarios del sistema • Falta de capacitación informática. • Desconocimiento de manuales de usuario. 	<ul style="list-style-type: none"> • Inadecuada ubicación de los equipos en el edificio de funcionamiento • Desconocimiento del plan de contingencia actual por parte del personal • No disposición de un plan de contingencia adaptado a la sucursal. • Falta de entrenamiento para el manejo de extintores. • Desconocimiento del

<ul style="list-style-type: none"> • Se observa coherencia de cargos. • Muy buena organización de la información. • Buena seguridad lógica de los datos. • Buen funcionamiento de la red. 	<p>al aceptar las sugerencias en cuanto a:</p> <ul style="list-style-type: none"> – Capacitación informática del personal. – Impartir un curso de Relaciones Humanas. – Entrenamiento en el uso del sistema actual. – Prevención de fallas eléctricas. – Entrenamiento en el manejo de extintores – Mejorar las relaciones laborales entre técnicos y usuarios del sistema, para evitar la omisión de requerimientos a la hora de diseñar y rediseñar el sistema. – Ejecutar un estudio de seguridad física en los archivos de la sucursal. – Contar con un plan de adquisiciones. 	<p>plan de contingencia actual.</p> <ul style="list-style-type: none"> • Insatisfacción del socio hacia la atención que recibe por parte de los empleados de OSCUS. • Ausencia de un suministrador de energía en el caso de apagones.
---	--	---

Fuente: Socios encuestados de OSCUS
Elaboración: Silvana Monge

3.10.3.2 INFORME DE TAREAS CUMPLIDAS DEL PLAN PARA EVALUAR RECURSO HUMANO

Dentro del plan establecido la primera tarea fue realizar una visita a la sucursal Latacunga, tarea que fue cumplida en un 100%, así como los objetivos propuestos para esta actividad como son el de observar el número de puestos de trabajo, necesidad de existencia de los mismos, número de empleados por puesto de trabajo.

La siguiente tarea cumplida fue la revisión de los curriculums de los empleados que son usuarios del sistema, con el objetivo de determinar su nivel profesional, además determinar si su formación académica corresponde a su asignación de trabajo. Como se observa en el anexo número 16, presentado en el CD de apoyo.

Al revisar los contratos de trabajo, determinando las observancias de derechos y obligaciones del empleado, se dio por cumplida esta tarea.

Lamentablemente por políticas de seguridad y obtención de copias de documentos privados no fue posible obtener copias de los contratos de trabajo de los empleados, por lo tanto no se logró cumplir con esta tarea. También fue posible determinar el nivel jerárquico y funcional de los empleados.

3.10.3.3 INFORME DE TAREAS CUMPLIDAS DEL PLAN PARA EVALUAR HARDWARE Y SOFTWARE

La primera tarea cumplida es esta etapa fue la vista a la sucursal Latacunga, para la constatación física del estado de los equipos, llegando así a alcanzar con los objetivos planteados.

La segunda tarea que consistía en diseñar y elaborar un sello adhesivo para constatación de la verificación física de los equipos, fue cumplida como se muestra en el CD de apoyo anexo número 17, así también de un certificado que avalice la revisión física de los equipos por parte del auditor. Como se puede ver en el anexo número 18, contenido en el CD.

Otra tarea cumplida fue la instalación de un software denominado Task Info para monitorear el recurso hardware utilizado. Obteniendo resultados como se observa en el CD de apoyo anexo número 19.

Con el cumplimiento de las tareas anteriores fue posible armar un inventario que ayuda a la presentación del recurso hardware y software del que Oscus Sucursal Latacunga dispone, como se puede ver en el anexo número 25, en el CD de apoyo.

3.10.3.4 INFORME DE TAREAS CUMPLIDAS DEL PLAN PARA EVALUAR COMUNICACIONES

El primer paso en la evaluación de la red es la obtención del diseño de la red el cual fue facilitado por el jefe de informática, mismo que consta en el anexo número 26, contenido en el CD de apoyo.

Otra tarea cumplida fue la instalación del software denominado Network Inspector con el objetivo de determinar la existencia de una red. Como se muestra en el anexo número 27, dentro del CD.

Además se instaló un software que permite la obtención de la gráfica de la red instalada, este programa se denomina Network Diagram, como se observa en el anexo número 30, en el CD de datos.

El siguiente paso es evaluar la ubicación de los terminales, monitoreando los flujos de información mediante la instalación del software denominado Ethereal y los anchos de banda ocupados por Oscus con el software de monitoreo denominado PRTG Traffic Grapher. Cuyos resultados se pueden observar en los anexos 28 y 29. en el CD de apoyo.

3.10.4 INFORME DE CUMPLIMIENTO DE ACTIVIDADES DE LA FASE IV



UNIVERSIDAD TECNICA DE COTOPAXI



INFORME DE CUMPLIMIENTO DE FASE VI

TEMA TESIS: Auditoria Informática en la Cooperativa de Ahorro y Crédito

Oscus Ltda. Sucursal Latacunga

AUTOR: Silvana Monge

DIRIGENTE: Ing. Emma Campaña

TEMA: Comunicación de resultados.

Objetivos: Para esta fase se han planteado los siguientes objetivos:

- Estructurar el informe final
- Diseñar y entregar convocatorias a lectura del informe final
- Lectura del informe final
- Ejecutar correcciones.
- Obtener el informe final de auditoría.

Esta fase es la final de auditoría informática, es la que se prepara el informe final, la lectura del mismo, para lo cual se realizaron invitaciones a los directivos de

Oscus y al director de proyecto, por lo tanto todas las tareas planificadas para esta fase se dieron cumplimiento incluido las correcciones respectivas por parte de los directivos, hasta llegar a obtener un informe final como se muestra a continuación:

3.11 ANÁLISIS DE LA INFORMACION OBTENIDA EN EL CUMPLIMIENTO DE LAS TAREAS.

3.11.1 ANALISIS DE LA FASE I

El principal objetivo de la fase preliminar es obtener información previa del estado de las institución, esta fase ayuda a generar horizontes que guíen a la siguiente fase mediante la determinación de la conveniencia de seguir o no con el ejercicio de auditoría en este caso de acuerdo con la información obtenida en la mencionada fase es conveniente realizar auditoría informática por las razones que a continuación se describen, presentándolas como un análisis de fase:

Una de las razones y quizá la más importante es la ausencia de auditoría informática puesto que cuando se aplico el formulario de guía de visita previa se pudo determinar que en esta sucursal no se había realizado este tipo de auditoría.

Al aplicar la técnica de verificación ocular en las visitas personales que se realizaron a la sucursal Latacunga, se logró determinar que en dicha institución se cuida de la seguridad del equipo y personal, mediante un guardia de seguridad, con esta medida se está cumpliendo con políticas de seguridad, así como la norma

400-09 de la Contraloría General del Estado, con título: Seguridad General en los Centros de Procesamiento de Datos, en el que manifiesta: se establecerán mecanismos que protejan y salvaguarden a equipos y programas.

En el recorrido por las instalaciones, aplicando la técnica del rastreo, en cuanto a ubicación de equipos se refiere se determino que el servidor se encuentra instalado en el área de cajas contando con poca seguridad física tomando en consideración que el servidor es un terminal de vital importancia para el funcionamiento del sistema instalado en Oscus, aplicando la misma técnica se establece que la sucursal está dividida en salas de trabajo las mismas tienen funcionalidad es decir secretaria se encuentra cerca de gerencia, por la estrecha relación entre las funciones de estos departamentos, el área de cajas está ubicado en la planta baja de la sucursal facilitando el ingreso de los socios, las salas de contabilidad, crédito y notificaciones funcionan en la segunda planta obteniendo cierta privacidad y quietud para el cumplimiento de las actividades por su poco contacto con el público, siguiendo con el rastreo en la visita a oscus, se observa que en la sala destinada a comunicaciones, no posee una puerta con chapa y se controla la seguridad con un ángulo corto de alcance de la cámara de vigilancia ubicada sobre la puerta posterior de la planta baja, para examinar este punto se aplica la técnica de comparación es decir que al comparar el beneficio que se obtiene al dotar a la sala de comunicaciones de una chapa o aldaba con candado, ante la vigilancia de una cámara, que graba y registra los sucesos, pero la dificultades de abrir un seguro en la puerta es ventajoso, lo mejor sería la combinación de las dos medidas de seguridad.

Siguiendo con el recorrido dentro de la sucursal y aplicando la técnica de verificación ocular, se logró verificar el buen estado físico de los equipos, la operatividad de los mismos, el número de equipos en cada sala es el adecuado es decir uno en cada sala, más el servidor haciendo un total de 7 computadores, existiendo una adecuada distribución de equipos, cumpliendo así con la norma 400 – 11 con título: Aprovechamiento de los recursos computarizados.

Al aplicar la técnica denominada revisión selectiva, se comprobó la existencia de documentos en donde se pone de manifiesto la organización de la sucursal segregando funciones, estableciendo jerarquías, en cuanto a la documentación de contratos de trabajo se toma en cuenta la necesidad de vacaciones y en el caso de personal femenino horas de lactancia y maternidad, cumpliendo así con las políticas de la cooperativa, la política que no se ha dado cumplimiento es la capacitación del personal que labora en la sucursal especialmente capacitación informática, siendo esta una desventaja para la institución.

Cuando se aplico la técnica de entrevista al Gerente de la sucursal se lego a establecer que en la sucursal existe un mecanismo para dotar de energía alternativa en caso de fallo, pero al compararlo con la observación directa se determinó que no es así, la sucursal carece de prevención en caso de falta de energía eléctrica.

En referencia al área informática en las visitas que se hicieron a la misma fue posible constatar la observancia de seguridades tanto en el edificio como en el

departamento de sistemas, especialmente en el área de servidores, controlando temperatura tención eléctrica, y restricción de acceso, cumpliendo así con la política interna de seguridad.

Aplicando la técnica de revisión selectiva se constató que el área de sistemas está bien definida estableciendo funciones, jerarquías y responsabilidades, como se puede apreciar en el anexo número 8, entonces se puede concluir que el área está organizada estructural y funcionalmente, cuando se ejecuto la técnica de rastreo del proceso de cumplimiento de responsabilidades fue posible establecer que se respeta las funciones, jerarquía de cada empleado dentro del área informática.

Al aplicar la técnica de observación se comprobó el buen estado físico y operatividad de los equipos, así como la inexistencia de subutilización de equipos, además estos están ubicados adecuadamente distribuidos en salas de trabajo como la de desarrollo en la que se hacen las pruebas antes de implantar cambios en el sistema.

La observancia de medidas de seguridad es buena, puesto que para permitir el ingreso al área informática en especial a las salas de producción, servidores y archivo se hace necesario una autorización de gerencia general o a su vez del jefe de área, como política de seguridad el personal debe acompañar siempre al visitante, además debe registrar su visita en un registro en recepción.

En la revisión selectiva de los contratos de mantenimiento se pudo determinar la existencia a de tal documento, como política interna al realizar mantenimiento de los equipos el personal de la empresa contratada no puede ingresar con equipo extraño o con maletas que no sean necesaria para la ejecución del trabajo.

En la técnica revisión selectiva, se evaluó el objetivo de Oscus que es llegar al 100% de automatización de todos los procesos de la cooperativa y al tratarse de un sistema joven aún no cubre todos los proceso pero se han automatizado la mayoría de ellos especialmente los de vital importancia como los procedimientos de área contable, análisis de crédito, recepción y egreso de capitales por cajas, etc. que dando por automatizar pasos complementarios.

El personal que labora en el área informática está capacitado, conoce de programación, todo esto se ve reflejado en el desarrollo interno del sistema que emplea Oscus, como manifiesta en la entrevista ejecutada al jefe de área.

En la revisión selectiva de la documentación de un plan de actividades se observó que constaba en dicho plan una actividad en la que se capacitaría a nivel informático al personal que labora en las diferentes sucursales, pero al comparar este dato con las investigaciones en la sucursal dicha actividad no se ha cumplido.

Luego de este análisis se puede concluir que la ejecución de auditoría informática es conveniente puesto que en el desarrollo de la fase preliminar se hallaron aciertos y errores que ameritan la investigación más profunda de los mismos.

3.11.2 ANÁLISIS DE FASE II

El objetivo Principal de esta fase es indagar sobre el de los recursos informáticos disponibles en la Sucursal Latacunga, entendiéndose por recurso informático, al sistema, el recurso humano, las comunicaciones (red), el hardware y software. De esta investigación resultará la determinación de áreas críticas.

Mediante la aplicación de un cuestionario de control interno, aplicado tanto al gerente de sucursal como al jefe de área informática, en lo referente al punto de energía suplementaria se determina que existe información contradictoria entre las dos partes interrogadas, además en una de las visitas a la sucursal fue posible constatar directamente la ausencia de prevención en caso de fallo eléctrico puesto que por mal tiempo se cortó el suministro de energía eléctrica en la ciudad de Latacunga viéndose afectados los equipos; con estos datos y acontecimientos se comprueba que la sucursal Latacunga no pose energía alternativa que permita seguir operando con normalidad.

Otro punto tomado en cuenta en el cuestionario de control interno fue la observancia de seguridades con respecto a equipos y personal en caso de incendios, este fue comprobado utilizando las técnicas de verificación física y ocular es decir que a más de la declaración verbal por parte del entrevistado, se confirmó la existencia de medidas de prevención de incendios como extintores, alarmas contra incendios, políticas de uso de equipos, organización de materiales de oficina, también mediante la verificación ocular fue posible comprobar que las

instalaciones eléctricas no tengan contacto con material combustible, inexistencia de letreros con prohibiciones de fumar o ingresar con material pirotécnico, todas estas medidas son indispensables para prevenir incendios puesto que la información contenida tanto en la sucursal como en la matriz es sumamente importante.

En el cuestionario de control se tocó el tema de la existencia de un manual de usuario que facilite el uso del sistema en operación pero la negativa se hizo presente, para verificar este dato, se aplicó la técnica de verificación verbal preguntando a los empleados si tenían conocimiento de un manual de usuario, obteniendo una respuesta negativa, también al aplicar la técnica de verificación documental se confirmó la inexistencia de este documento en la sucursal, pero al interrogar sobre este punto al jefe de informática presentó dicho documento pero este no había sido distribuido al personal que labora en la matriz ni en las sucursales, entonces de este análisis se desprende la conclusión de que el personal de oscus no tiene conocimiento, no posee un manual de operación del sistema.

La seguridad física en el área de informática es buena, puesto que mediante la aplicación de la técnica de verificación ocular se pudo evaluar este punto determinando que el acceso al área es restringido, en la sucursal en cambio el acceso al público no es restringido por las actividades que en ella se cumplen como depósitos, retiros, solicitud de préstamos, apertura de cuentas, etc. pero existe un guardia de seguridad.

Las condiciones ambientales son agentes para posibles daños en los equipos por lo que se vigila constantemente, temperatura, ventilación, iluminación, etc. del área informática situación que se constató aplicando la técnica de verificación física, observando la existencia de termómetros, ventiladores, utilización de multimetros, etc. en la sucursal Latacunga la evaluación de este control no fue necesaria porque las condiciones ambientales en sí dentro del edificio son adecuadas, además no existen salas de cuidado como en el caso del área informática la sala de servidores.

Para el examen del sistema se aplicaron técnicas como verificación verbal, documental y escrita, es así que al interrogar al jefe de área, acerca del control de seguridades en el sistema, controles de confiabilidad de de los datos que son ingresados al sistema, etc. manifestó que cada usuario cuenta con una clave personal que se debe cambiar cada tres días o cuando el empleado crea que su clave ha sido descubierta, el aviso de requerimiento para cambiar la clave se genera automáticamente, en el caso de intento fallido de ingresar al sistema por parte de personal no autorizado, se bloquea el sistema al tercer intento fallido y el incidente tiene que ser reportado a soporte técnico para lograr desbloquear el sistema, para la comprobación de este control se evaluó mediante la comprobación directa con la manipulación del sistema, obteniendo la conformación positiva de la información brindada por el jefe de área. También en el sistema se establecen niveles de acceso de acuerdo con las actividades de cada usuario. Mediante la aplicación de la técnica de verificación documental se pudo

comprobar la existencia de manuales de programación, normas de programación, etc. que regularon el diseño, desarrollo e implementación del sistema.

Otro punto que fue posible analizar mediante la verificación documental es la existencia de un plan de contingencia que ayuda al control de actividades, antes, durante y después de un desastre, pero lamentablemente al solicitar este tipo de documento en la sucursal se comprobó la inexistencia del mismo, de modo que el personal no está preparado para actuar en caso de desastres.

El área de sistemas está regulada por políticas internas contenidas en un documento, que se lo evaluó mediante la técnica de verificación documental, las políticas se refieren a seguridad física, liberación y respaldo de la información, control de acceso al área de procesamiento, mantenimiento de hardware, software y sistema, esta última política guía los procedimientos de mantenimiento del equipo.

Al interrogar al jefe de área si se controla el uso que se da a los terminales por parte de los empleados la negativa se hizo presente, en cuanto a comunicaciones mediante la verificación física se logró determinar que las comunicaciones se realizan mediante módems y con líneas dedicadas.

En cumplimiento con los pasos de la metodología de auditoría informática se analizó los datos obtenidos como consta en las páginas anteriores, determinando errores significativos encontrados y errores no significativos que se apuntan en

una carta a gerencia con la sugerencia para mejorar estos errores, dicha carta consta en el anexo número 11, contenido en el CD de apoyo

3.11.2.1 DETERMINACIÓN DE AREAS CRÍTICAS

Después de la obtención de información y el análisis de la misma en la fase II, es posible determinar áreas críticas que requieren ser examinadas en la siguiente fase; estas áreas son:

SISTEMA: Pese a que en esta fase no se ha encontrado inconvenientes es necesario examinar detenidamente aspectos como estudio de factibilidad, diseño, desarrollo, e implementación del sistema así como los procedimientos que se siguen para modificaciones en el programa. Por estas razones se considera y establece como un área crítica al sistema implementado en Oscus.

RECURSO HUMANO: Dentro del desarrollo de la fase II, se determinó que el personal de la sucursal Latacunga, no está entrenado para determinación de fallas o averías en su equipo, o del manejo de los programas disponibles.

Es necesario investigar sus Curriculums para determinar la coherencia o incoherencia de cargos, etc. por todos estos motivos la segunda área crítica a inspeccionarse es el recurso humano de la sucursal Latacunga.

HARDWARE Y SOFTWARE: en la fase II al descubrir que no se realizan inspecciones del uso que se esta dando al software y hardware se hace indispensable sondear con detenimiento el recurso hardware y software disponible en la sucursal, de este modo se establece la tercera área crítica: hardware y software que posee Oscus sucursal Latacunga.

COMUNICACIONES: Un área sin duda crítica dentro de una institución que depende de otra como en este caso la sucursal depende de la matriz, es innegable la exigencia de valorar el funcionamiento de la red de que dispone la institución, puesto que para ofrecer un buen servicio a los socios las interconexiones internas y externas son esenciales.

3.11.3 ANÁLISIS DE FASE III

Esta fase tiene por objetivo primordial la evaluación más detenida de las áreas críticas determinadas en la fase anterior, el examen está organizado por segmentos, para al final obtener una valoración general del estado de la sucursal Latacunga, acotando con algunos puntos del área de informática.

3.11.3.1 EVALUACIÓN DE RECURSO SISTEMA

Mediante la aplicación de la técnica de interrogación o entrevista se aplicó un test al jefe de área informática. Cuyo detalle se encuentra en el anexo número 13,

contenido en el CD de anexos. El sistema que se emplea en Oscus como ya se dijo anteriormente fue desarrollado internamente, con la gran ventaja de quienes lo crearon conocen de las necesidades de los usuarios, además ganan licencia ilimitada de uso, dicho sistema se denomina Sifiz Os, de este es un sistema centralizado de éste dependen todas las sucursales como las de Pelileo, Patate, Pillaro y Latacunga. El sistema implementado en Oscus se evaluó de acuerdo con el ciclo de vida que normalmente siguen los sistemas: requerimientos del usuario, estudio de factibilidad, diseño general, análisis, diseño lógico, desarrollo físico, pruebas, implementación, evaluación, modificaciones, instalación, mejoras.

La primera etapa a evaluar del sistema es el estudio de factibilidad, el cual debe analizar si el sistema es factible de realizarse, cuál es su relación costo/beneficio y si es recomendable elaborarlo. Para lo cual se aplicó la técnica de observación documental, mediante la cual se pudo constatar la existencia de este documento y al evaluarlo se verificó este es un documento legal registrado ante la notaria primera de Ambato del Sr. Abogado Naranjo, en el que se celebra un contrato de creación de Software entre el Gerente General Sr. Ing. Edgar Pazmiño y el Sr. Ing. Ing. Tomás Zules Ramires, en el mencionado contrato se establecen cláusulas como el derecho intelectual por parte del dirigente del proyecto. Con este contrato se verifico la legalidad que avaliza la creación del software.

También se constató mediante la técnica de confirmación que en el estudio de factibilidad se cumplió con los pasos, para desarrollar un estudio de viabilidad o factibilidad; pasos como:

Antecedentes, Objetivos, Costos, Beneficios, Herramientas de Desarrollo, Etapas de desarrollo de proyecto, requerimiento Humano, Requerimiento Software.

Los beneficios justifican el desarrollo del sistema, ya que ahorran los costos de operación, se obtiene reducción del tiempo de proceso de un sistema con mayor exactitud, mejor servicio, presentando mejoría en los procedimientos de control, mayor confiabilidad y seguridad, en comparación con el sistema anterior que venía funcionando en Oscus. Además por tratarse de un sistema diseñado internamente con los requerimientos de los usuarios y con el beneficio de la exclusividad del mismo.

Debo anotar que por razones de confidencialidad de la institución y políticas de Seguridad del Área de Sistemas, no fue posible obtener una copia de este documento, en su defecto la constatación de su existencia y la lectura del mismo bastaron.

3.11.3.1.1 EVALUACIÓN DEL DISEÑO LÓGICO DEL SISTEMA

En esta etapa se analizó mediante la observación documental, verificación directa, las especificaciones del sistema, como por ejemplo el manual de usuario, el manual del programador, manual de formas, etc.

Para la evaluación del diseño del sistema fue necesario determinar, si los programadores y analista de sistemas contaban con una guía que les permitiese

diseñar el sistema, además, se analizó si se sigue un procedimiento, como son las graficas de flujo de información, etc.

Entonces para el diseño del sistema, se determinó mediante verificación documental que en el área de sistemas existe un manual de diseño, programación e implementación de sistemas, que sirvió de guía para el desarrollo del sistema a más del jefe de proyecto que fue la cabeza en la planeación y ejecución de Sifiz Os.

En cuanto a procedimiento: En el diseño del sistema interviene lógicamente el director de proyecto en este caso el Ing. Tomás Zules Ramires, como programador y analista el Ing. Carlos Santamaría en calidad de Jefe de Área, como programadores el Ing. Francisco Lozada y el Ing. Juan Freire, este grupo de trabajo se estableció un tiempo de ejecución del trabajo de 6 meses, para el diseño del sistema se sirvieron de Normas para el Desarrollo y Mantenimiento de Código.

Al igual que en el paso anterior por políticas de seguridad del Área de Sistemas, no se logro obtener una fotocopia de las Normas para el Desarrollo y Mantenimiento de Código, pero en la constatación documental se pudo observar que se seguían normativas como: reglas para clases, reglas para interfaces, reglas para campos, parámetros, guías para la creación de clases, uso de constructores, tipo anidados, tipo valor, etiquetas recomendables para documentos código, normas para archivo de código fuente, declaración de clases e interfaces.

En la gráfica de flujo de información: En cuanto a la grafica del flujo de la información propuesto en los modelos entidad relación de las Bases de Datos, fue posible determinar que es fácil de usar, que se han seguido las formas normales, en especial primera segunda y tercera forma normal, tiene lógica de estructura y flujo de información, está bien estructurando eliminando la presencia de lagunas y fallos de control.

En el diseño: En cuanto al diseño del sistema, mediante observación documental fue posible determinar que los creadores del mismo realizaron un diseño contemplando objetivos que persigue el sistema, recursos, hardware, software, por adquirir, disponibles y reutilizables, recurso humano; además realizaron una estimación del proyecto.

También se determinó que para el diseño del sistema se utilizaron técnicas y herramientas adecuadas, como por ejemplo: el modelo COCOMO, estas herramientas se ajustan al desarrollo del sistema.

De esta constatación documental y física se deduce que para el diseño de SIFIZos se estableció un grupo de trabajo, se observaron normativas de diseño, se aplicaron técnicas, procedimientos de diseño, estimación, lo que hace que SIFIZos, esté funcionando actualmente, satisfaciendo los requerimientos del usuario final que es el juez más preciso a la hora de pruebas de ejecución de sistema.

3.11.3.1.2 EVALUACIÓN DEL DESARROLLO DEL SISTEMA

En esta etapa se auditaron mediante la aplicación de observación escrita y documental los programas, su diseño, el lenguaje utilizado, y características del hardware empleado para el desarrollo del sistema.

Al inquirir en las herramientas utilizadas para el desarrollo de sistemas se verifico que se usó DOT NET de Microsoft, con lenguaje de programación C Sharp, en un ambiente WEB.

Para el desarrollo de la Base de Datos se usó SQL Server de Microsoft. La plataforma de trabajo obliga a trabajar en un ambiente totalmente Orientado a Objetos.

El Fron end se presenta en ambiente Internet, utilizando Internet Explorer, como herramienta para acceso a páginas por parte del usuario de todas las oficinas de la Matriz y Sucursales.

Al evaluar el sistema de información se determinó que está organizado y controla de manera eficaz y oportuna la reducción de duplicidad de datos. Además brinda una mayor seguridad en la forma más económica posible.

Al aplicar accesos y claves, se puede decir que se observa la seguridad de movimiento de la información entre nodos.

También se puede decir que el sistema es dinámico es decir susceptible a modificaciones y de echo siempre se está modificando de acuerdo a los requerimientos de los usuarios del sistema.

Dentro de una de las aplicaciones el sistema permite controlar que los datos que entrega el cliente, especialmente en la apertura de cuentas, en lo que tiene que ver a número de cédulas, en el sistema existe una aplicación que permite conectarse con la pagina de registro civil y determinar si el número de ciudadanía entregado por el socio es el correcto.

Las interacciones de sus componentes o subsistemas actúan como un todo, es decir el sistema es estructurado, mostrando ser un programa integrado, con un solo objetivo, sin programas aislados.

El sistema es disponible es decir muestra accesibilidad, también es necesario, puesto que se verificó la utilización del mismo, legando a determinar que en todas las terminales de la matriz y la sucursal Latacunga se utiliza este sistema para las labores diarias.

Las interfaces con las que se presenta al usuario final son amigables, de fácil utilización, la información esta disponible en el momento que se requiere, es decir el sistema es oportuno.

La información que proporciona el sistema como consultas, reportes, movimientos, contabilización de roles, liquidación de haberes, liquidación de préstamos, etc. es adecuada para cada nivel, por lo tanto el sistema es funcional.

La capacidad de modificación que tiene el sistema para cada requerimiento del usuario, y de la Superintendencia de Bancos, habla de su modularidad, puesto que tiene facilidad para ser expandido o reducido.

En cuanto a accesos, orientación de trabajo en ambientes diferentes o niveles funcionales, como de gerencia, cajas, contabilidad, secretaria, se puede decir que el sistema cumple con el requerimiento de jerarquía.

El sistema denominado SIFIZos, emplea claves de acceso, con claves unipersonales para cada ambiente de trabajo, cuando el usuario comete tres errores en el ingreso de la clave el sistema se bloquea, por lo tanto el sistema observa medidas de seguridad, esto fue posible determinar mediante la constatación directa manipulando el sistema.

Con este amplio análisis se deduce que el desarrollo del sistema esta bien orientado con las herramientas y normativas necesarias para la ejecución del desarrollo de sistemas.

3.11.3.1.3 EVALUACIÓN DEL CONTROL DE DISEÑO DE SISTEMAS Y PROGRAMACIÓN

El objetivo es asegurarse de que el sistema funcione conforme a las especificaciones funcionales, a fin de que el usuario tenga la suficiente información para su manejo, operación y aceptación.

Esta actividad es muy importante ya que el costo de corregir errores es directamente proporcional al momento que se detectan: si se descubren en el momento de programación será más alto que si se detecta en la etapa de análisis.

Después del diseño lógico de sistemas y programación viene la ejecución, para lo cual se constató que en el área de sistemas siempre el Jefe de área esta presente supervisando, dirigiendo y vigilando el trabajo de los analistas y programadores.

Para el control del diseño de sistemas y de programación se constató que el grupo de trabajo estudia el diseño lógico, discute con el analista, codifica, compila, corre programas con datos, documenta el programa y el código fuente, somete los resultados a prueba, antes de implementarlo o presentarlo para el uso de los empleados de Oscus.

3.11.3.1.4 EVALUACIÓN DE LA FORMA DE IMPLEMENTACIÓN

La finalidad de evaluar los trabajos que se realizan para iniciar la operación de un sistema, esto es, la prueba integral del sistema, adecuación, aceptación por parte del usuario, entrenamiento de los responsables del sistema etc.

Luego del diseño, desarrollo de SIFIZos, sobrevino la implementación, para lo cual se realizaron en primera instancia pruebas del sistema, estas pruebas se realizaron en cuatro paralelos, con las pruebas listas y las adecuaciones, correctivos aplicados, se procedió a la capacitación o entrenamiento del personal de Oscus, aquel que estaría directamente relacionado con dicho sistema.

3.11.3.1.5 EVALUACION DE LA BASE DE DATOS Y CODIGO FUENTE

La Base de Datos creada en SQL de Server de Microsoft, el lenguaje de programación que utilizaron fue el C# Sharp orientado a Internet, fue posible determinar que no existe over flow, o sobre flujo de datos.

La Base de Datos cumple con la normalización, esta documentada, el modelo entidad relación esta bien diseñado, organizado, no hay sobre carga de información en la base de datos que altere su funcionamiento, la plataforma de lenguaje de programación, el lenguaje y los requerimientos obligan a trabajar en un ambiente web. Orientado a Objetos y con herramientas Internet por lo tanto el enlace usado es .NET .

Todo el sistema esta programado en lenguaje C# Sharp, el código está documentado para reprogramación y mantenimiento, este código es dinámicos es decir susceptibles a modificaciones, además las interacciones de sus componentes o subsistemas actúan como un todo integrados en un solo objetivo.

Se puede decir con seguridad que este código es comprensible conteniendo todos los atributos, el diseño y codificación permite obtener información adecuada a cada nivel y en el momento que se requiere.

Debido a que el sistema esta orientado a las necesidades del usuario, el código es modular es decir tiene facilidad para ser expandido o reducido, además observa niveles de acceso y seguridad lógica para el ingreso al sistema, también se cuida en el código que no se duplique la información y se valida el ingreso de datos.

Al revisar el manual de usuario se logró determinar que es de fácil uso, que tiene un ambiente gráfico, detallando paso a paso el funcionamiento del sistema, pero lamentablemente, el mismo no ha sido distribuido a los usuarios del sistema como lo manifiesta en la entrevista al Gerente de la Sucursal Latacunga, incumpliendo así con la política de entrega de documentos afines al sistema , al leer el plan de contingencias se pudo detectar que el mismo se toman en cuenta las actividades previas durante y después de un desastre con la evaluación de daños y las acciones a tomar, pero no existe un plan de contingencias adaptado a la sucursal tomando en cuenta que esta es una alternativa para el funcionamiento de Oscus en caso de falla de la matriz como consta en el plan de contingencias.

En el plan de contingencias se observan las medidas de seguridad física, lógica y confidencial cumpliendo con las políticas de: Uso de claves y usuarios confidenciales, actualización de de versión del aplicativo y base de datos, para la liberación y respaldo de información de la Base de Datos.

Al analizar los reportes generados por el sistema se puede decir que estos son útiles para contabilidad.

Los empleados obtienen reportes diarios los cuales son impresos y transferidos a contabilidad, los reportes generados en cajas ayudan al control de ingresos, egresos, efectivización de cheques, arquezos de cajas, etc. Se puede decir que los reportes son necesarios, contienen los datos correctos e indispensables para el funcionamiento de la institución especialmente a nivel contable.

Aplicando la técnica de verificación documental se determinó que para el diseño del código fuente se utilizó la normativa para mantenimiento y desarrollo de código, en la que se especifican todas las normas de programación, el trabajo de los analistas y programadores se lo controla mediante pruebas piloto que se ejecutan en el área de producción, es decir antes de la implantación de una modificación al sistema se corren los programas, se revisan los resultados, se documenta el programa, si los cambios son significativos, se obtiene un respaldo del sistema actual para comparaciones y corrección de errores, según política la puesta en línea de nuevas versiones. Entonces se concluye que el diseño de programación cumple con normativas, especificadas anteriormente.

El sistema que se utiliza en Oscus es en línea, es decir los usuarios capturan la información, pero el sistema valida esos datos, Además se establecen niveles de acceso mediante claves al sistema, por ejemplo el cajero no puede ingresar a datos del gerente, como el gerente no puede ingresar a datos de contabilidad, pero contabilidad es un administrador que requiere los datos de los demás terminales. Cumpliendo así con la política de seguridad lógica de los datos, y la política de uso y confidencialidad de password (claves)

En cuanto a cifras de control para archivar los respaldos que se realizan en forma diaria y mensual aplican la política de respaldo y liberación de información en la que se puntualizan las especificaciones de formato y sintaxis para las etiquetas de los respaldos. Es decir se da cumplimiento a la política de obtención de respaldos y etiquetado de los mismos, identificando cada cinta con la primera letra del mes, la del día de la mañana o tarde y la fecha de obtención de respaldo, esto fue posible determinar mediante la verificación ocular de las cintas, ubicadas en archivo.

También mediante la técnica de verificación ocular se legó a determinar que el área de archivo cuenta con seguridad, así como de instalaciones adecuadas para el almacenamiento de los respaldos, cumpliendo así con la política de de seguridad y control de acceso al área de procesamiento de datos.

Para iniciar las labores se realiza un backup de la información y otro al finalizar el día, así como los respaldos mensuales, en la bitácora que esta ubicada dentro del

área de informática, se almacenan estos datos, luego se los traslada a la bóveda de un banco para salvaguardar la información, cumpliendo con la política de respaldo y liberación de datos.

Los dispositivos de almacenamiento representan, para cualquier centro de cómputo, archivos extremadamente importantes cuya pérdida parcial o total podría tener repercusiones muy serias, no sólo en la unidad de informática, sino en la dependencia de la cual se presta servicio.

Por lo tanto en el área de informática existen normas preventivas y medidas de acción en el caso de producirse un incendio, como por ejemplo: alarmas contra incendios, detectores de humo, control de temperatura con termómetros en la sala de servidores, extintores de fuego ubicados en sitios estratégicos, es decir que son están colocados al alcance de los empleados, evitando de este modo la pérdida de tiempo valioso. Cumpliendo de esta manera con la política de seguridad y control de acceso al área de procesamiento de datos.

3.11.3.1.6 ANALISIS DE LAS APLICACIONES DEL SISTEMA

El sistema denominado Sifiz Os, esta diseñado y programado por módulos, estableciendo niveles de acceso mediante claves de acceso, dependiendo las tareas que va a desempeñar el usuario y el permiso que posee para ingresar a determinados datos, por ejemplo las tareas que ejecuta la secretaria de Oscus son muy diferentes a las de la contadora que a su vez difiere mucho del analista de

créditos, entonces se podría decir que representa una gran ventaja en cuanto a la privacidad de los datos.

Cada usuario tiene restringido el acceso a ciertas aplicaciones del sistema por ejemplo el analista de crédito tiene denegado el acceso a movimientos de capitales en cajas, así como el recibidor pagador no tiene acceso a movimientos contables. Cuando un usuario pretende ingresar a una aplicación que no le es permitida se despliega automáticamente un mensaje en el que le recuerda al empleado la restricción de uso de la aplicación, como se muestra en el anexo número 15 contenido en el CD de apoyo, cuando el auxiliar de notificaciones pretende ingresar a central de riesgos que es un reporte de datos financieros de los socios en otras instituciones bancarias, y al cual no tiene asignado roles es decir el acceso a esta aplicación esta restringido para las actividades de verificaciones de moras, notificaciones, etc. por tanto se puede decir que dentro del sistema se está cuidando la privacidad de datos estableciendo niveles de acceso niveles de acceso, situación que fue verificada aplicando la técnica de observación directa y manipulación del aplicativo.

Gerencia cumple funciones propias y compartidas por tal razón en el sistema también puede realizar consultas de préstamos, en las aplicaciones de cajas autorizaciones, esta capacitado para realizar reversos es decir cuando en cajas se realizó una transacción errónea, existe la posibilidad de anular dicho proceso, otra aplicación a la que tiene acceso el gerente es a transacciones internas es decir migración de capitales, transacción desde la cuenta al préstamo, de cuenta a

cuenta, también puede realizar consultas de saldos promedios, para conocer la fluctuación de capitales del socio en determinado período de tiempo, para establecer solvencia económica del mismo, el sistema le permite obtener un resumen de transferencias internas, saldos de captaciones, listas de cheque por efectivizar, consultar datos de socios, efectivizar cheques, autorizar desembolsos superiores a 2000, etc.

Dentro de las aplicaciones como ya se dijo anteriormente existe restricciones de acceso a las aplicaciones, es así que en cajas el recibidor pagador esta facultado para ejecutar algunas aplicaciones como en este caso: movimientos, cambio de cheques, cambio de efectivo, cajeros, reportes cajeros, afectaciones, únicamente el cajero principal tiene acceso a la aplicación arqueado de caja en la que se muestra la denominación de caja es decir el responsable, la denominación en monedas, total de encuadre, desencuadre es decir en esta aplicación se lleva un control del movimiento de dinero en cada cajero. La primera tarea que cumple en el sistema el recibidor pagador es la inicialización de caja en la que registra el inicio de actividades por cajero, generando fecha, hora de inicialización, permiso respectivo para ejecutar movimientos financieros, también en la aplicación pago de préstamo es posible visualizar datos como la identificación del socio, tipo de préstamo, denominación, número de préstamo, mora, interés, etc. datos que son indispensables para el control de la secuencia de cancelación de préstamo, también el sistema encuadra automáticamente los valores de depósito con el monto de cada pago, permitiéndole aceptar excedente y alertar en caso de faltante, lo que quiere decir que el sistema está validando cantidades, como política de la

institución no se debe mantener en caja, caja chica más de una determinada cantidad en efectivo, por lo tanto la cooperativa posee cuentas en los bancos Internacional y Guayaquil, entonces en el sistema se registra los depósitos en los bancos auxiliares; en una aplicación denominada registro de papeleta, en la aplicación movimientos el recibidor pagador está en la facultad de ejecutar transacciones de retiro o depósito de ahorros en efectivo o cheque, para cada transacción existe una aplicación diferente en la que se controla los montos a debitar es decir su disponibilidad, las cantidades permisibles de retiro vía cajas, de lo contrario el sistema alerta sobre la necesidad de autorización de gerencia en montos mayores, en este tipo de aplicación el recibidor pagador registra las cantidades de ingreso con las denominaciones de cada depósito, en conclusión las aplicaciones destinadas a cajas están bien orientadas a las necesidades del operador del sistema y usuario, controla, valida, datos y cantidades, no se ha podido observar inconsistencia de datos, se determina también la existencia de niveles de acceso incluso entre cajas.

Para la ejecución de las tareas del analista de crédito están destinadas algunas aplicaciones, como por ejemplo la aplicación caja, en la que el analista está facultado para realizar autorizaciones de retiros por caja es decir en los montos que exceden a los 2000 dólares, esta función no le compete al cajero pero si al gerente, la que quiere decir que en el sistema se establecen rangos de accesos a las aplicaciones en torno a las funciones que desempeña cada empleado tanto de la matriz como de las sucursales, dentro de esta aplicación es posible validar el monto a retirar comparándolo con el disponible, si el monto excede al existente no

se genera la autorización, observando así seguridades en movimientos, dentro de captaciones el analista de crédito esta facultado para ejecutar desencajes, puesto que en esta aplicación visualiza el tipo y estado del préstamo para determinar si amerita el desencaje, en la aplicación préstamo el analista de crédito puede realizar solicitudes de préstamos, garantías, micro créditos, consultas, resoluciones, generación de préstamos, etc. en este menú dentro de solicitudes de préstamo en base al ingreso del monto requerido el sistema genera automáticamente datos como encaje, valor de cuotas, deuda inicial y monto a pagar, también puede realizar ingreso y levantamiento de garantías en función de la cancelación del crédito, es decir el sistema esta controlando la ejecución de esta aplicación siempre y cuando se haya cancelado el préstamo, para consultar estado de préstamos, historial del cliente se lo ejecuta mediante el número de cuenta o la identificación o cédula del socio, en cuanto a los reportes que genera esta aplicación está clientes, fin del día, jurídico, etc. estos reportes le permiten al analista de crédito obtener listas de los créditos entregados, con el tipo, monto, cliente, también es sumamente importante el reporte de riesgo puesto que en este se basa al analista para determinar el grado de morosidad. Otra actividad que cumple es la consulta del estado de créditos en proceso es decir cómo se encuentra cada crédito, las solicitudes revisadas pasan a una instancia denominada revisión, luego de un batch en verificación, pasa a otra instancia denominada verificada, se ejecuta otro batch, para ser aprobada y finalmente se produce el desembolso por caja.

El verificador puede obtener reportes de riesgo, consultas de créditos en proceso judicial, generación de esquelas para citaciones a socios morosos, consultas de estado de créditos, consultas de estado de solicitudes de crédito, historial de clientes e historial de créditos, consultas de créditos entregados por día, etc.

Una de las funciones que cumple la secretaria es la apertura de cuentas, o socios nuevos en donde se recopilan datos como: nombres, apellidos, número de identificación o cédula, dirección, teléfono, estado civil, profesión, número de cargas, No de cliente, que se genera automáticamente y es una de las directrices para evitar la duplicación de cuentas, que también es controlado automáticamente por el sistema, etc. para verificar si el número de es el correcto el sistema puede enlazarse con el TSE para verificar la existencia de esta cédula, otro modo de comprobar si el cliente es confiable, la aplicación CONSEP (Consejo Nacional de Sustancias Estupefacientes y Psicotrópicas) en el que se muestra una lista de las personas que tienen problemas con sustancias estupefacientes o psicotrópicas, esta consulta se la realiza a través del apellido.

Para el área contable la contadora esta facultada para realizar comprobantes, mayorización, plan de cuentas, fin del día de de oficina, proveedores, activos fijos, proveeduría, transacciones a SRI, puede realizar consultas de comprobantes, comprobantes en proceso, comprobantes de desencuadros, comprobantes de saldos de cuentas, listados de saldos de cuentas auxiliares y contables.

Mediante la ejecución del sistema, manipulación del mismo, comprobación de corridas de las aplicaciones con datos reales y ficticios fue posible determinar que las aplicaciones están funcionando correctamente que se están validando datos, estableciendo niveles de acceso de acuerdo a las funciones del empleado, no existe inconsistencia ni redundancia de datos, los resultados de las operaciones contables son correctos, es posible realizar reportes y consultas, no se observó fallos en los procesos, de lo expuesto se deduce que las aplicaciones son operativas.

3.11.3.2 ANALISIS DE EVALUACIÓN DEL RECURSO HUMANO

En la visita realizada a la sucursal Latacunga y aplicando técnicas como de rastreo, observación, se logró determinar que en la sucursal Latacunga no existen puestos fantasmas o inútiles, debido a que en cada departamento existe un empleado por puesto de trabajo, además que los empleados, según curriculum presentados, (anexo numero 16) se encuentran en el cargo adecuado concordando con el nivel académico, los puestos de trabajo son necesarios siendo estos: gerencia, secretaria, recibidor pagador, guardia, credito, notificación, contabilidad, mensajería, pero los curriculum revisados son aquellos que pertenecen a los empleados que son usuarios del sistema.

Aplicando la técnica de observación documental, en los contratos de trabajo, fue posible determinar que en estos consta el derecho a vacaciones, maternidad,

lactancia, etc. cumpliendo así con los reglamentos de la ley de contratación y código de trabajo.

Aplicado la técnica de interrogación y rastreo se siguió la línea jerárquica de Ocaso sucursal Latacunga, es así que la cabeza de esta es su gerente, en ausencia de este por diligencias fuera de la institución, vacaciones o calamidad doméstica, le sucede el analista de crédito, son subordinados los empleados de, contabilidad, secretaria, notificador verificador, receptor pagador. También fue posible determinar las funciones de cada así: Gerencia: Velar por el buen funcionamiento de la sucursal como cabeza de la misma, cumplir y hacer cumplir de todas las normas y procedimientos establecidos. Secretaria: Mantener toda la información de socios y del sistema, en orden y actualizadas, proporcionar información y servicio diligente a los socios. Contador:

El contador tiene como misión llevar la contabilidad de la sucursal Latacunga, mantener actualizada y en orden la información que se deposita en este departamento. Receptor Pagador: La función principal del receptor pagador es la atención al cliente cuando requiere realizar transacciones de depósito o retiro, este tipo de empleado es responsable del ingreso y salida de dinero así como de los arqueo de caja y obtención de reportes.

Analista de Crédito: La función principal del analista de crédito es la evaluación de las solicitudes de crédito, la aprobación o negación de las mismas, la vigilancia de las tasas de morosidad. Notificador Verificador: La función del notificador

verificador es la de realizar las inspecciones pertinentes con el fin de determinar la veracidad de los datos presentados en la solicitud de crédito, además reducir las tasas de morosidad con visitas y llamadas telefónicas a los domicilios para notificar al socio que está incumpliendo con los debidos pagos.

De lo que se deduce que la sucursal está estructurada jerárquica y funcionalmente, cumpliendo con los requerimientos de organización de una entidad legalmente constituida.

En la entrevista realizada al gerente de la sucursal se obtuvo información acerca del modo de contratación de los empleados siendo esta mixta es decir directamente con las personas, y por medio de terciarizadora en este caso los empleados de cajas y secretaria, otro dato que proporcionó el gerente es que se capacita a nivel informático al personal de oscus, respuesta que fue refutada por los empleados de la sucursal como lo muestra el cuadro estadístico numero 4, en el que el 71.42%, manifiesta que capacitación informática es deficiente, otro dato interesante es que al entrevistar al jefe de area de sistemas manifiesta que en el plan anual de actividades se palntea la tarea de capacitación informatica al personal de todas las sucursales, pero aún no se cumplido, por lo tanto la carencia de conocimiento informático en el personal que labora directamente con computadores es carente.

3.11.3.3 ANALISIS DE EVALUACIÓN DE HARDWARE Y SOFTWARE

Mediante la aplicación de la técnica de observación fue posible determinar la operatividad de las máquinas es decir todos los computadores de la sucursal Latacunga se encuentran funcionando, tienen un buen estado físico así como los cables de red y conexiones, acometidas eléctricas, también mediante observación y constatación física se pudo apreciar que los componentes concuerdan con las marcas.

Al aplicar observación documental se logró determinar que Oscus cuenta con licencias de operación para el software así: para Windows Server una licencia, Windows Xp 4 licencias, Windows 98 5 licencias, Office 97 seis, Office XP una, Norton Antivirus 10. Así mismo para determinar las características de hardware, conexiones, Sistema operativo de las máquinas, archivos abiertos, se instaló un software de monitoreo denominado TaskInfo cuyo análisis se presenta a continuación:

3.11.3.3.1 ANALISIS DE INFORMACIÓN OBTENIDA CON TASKINFO

TaskInfo es un utilitario que combina rasgos de gerente de la tarea e información del Sistema. Es posible visualizar tipos diferentes de información del sistema; ya sea bajo Windows 95/ 98/ y/o/ NT/ 2000/ XP en tiempo real. Todos los numerales de anexos a los que se hace referencia en esta sección se encuentran almacenados en un CD de datos como apoyo.

TaskInfo muestra información detallada acerca del sistema y todo proceso e hilas que están funcionando en él. La información se presenta en texto y forma gráfica de acuerdo al requerimiento. También permite copiar o guardar tal información en un archivo tipo HTML o tipo texto en Bloc de notas. Otra utilidad que se obtiene con este software es correr, detener procesos y cerrar por fuerza ciertos procesos, y reiniciar el sistema.

La información que se puede observar al obtener el resultado del monitoreo se divide en dos partes: Processes Pane (Panel de Procesos) y System Pane (Panel del Sistema). En **Processes Pane** (Panel de Procesos) visualizamos información como: identificación del proceso, detalle del proceso, uso del CPU, tiempo de uso de CPU, cantidad total de ejecución de cada proceso, cantidad de memoria física usada, cantidad de memoria virtual usada, cantidad total de la memoria virtual usada por los procesos, número de hilas corriendo, prioridad de los procesos, versión del Windows, número de objetos abiertos, tiempo de inicio del sistema.

En **System Pane** (Panel del Sistema) es posible obtener información sobre: el sistema en forma general, drivers, archivos abiertos, conexiones, sistema operativo y servicio de acceso remoto

3.11.3.3.2 ANALISIS DE LOS RESULTADOS OBTENIDOS EN

PROCESSES PANE (PANEL DE PROCESOS)

CAJERO PRINCIPAL

De lo observado es claro deducir que los procesos con mayor prioridad de ejecución son: Aplicación de inicio de sesión de Windows NT, TaskInfo Aplicación, cada una con prioridad alta, los procesos que utilizan mayor memoria física son: LSA Shell, con 2.504 KB; Explorador de Windows con 18.012 KB; en cuanto a memoria virtual se refiere los procesos son: Aplicación de inicio de sesión de Windows NT con 7.104 KB, Norton Antivirus con 37.244 KB, Virus Definition con 16.808 KB, Explorador de Windows con 92.888 KB. Con estos valores se puede concluir que la memoria física, virtual y la prioridad en este computador están bien encaminadas no se observa subutilización o la presencia de procesos ajenos a las necesidades laborales. Para mayores detalles ver anexo No 19 literal a.

CAJERO SECUNDARIO

En el computador designado para el cajero secundario el proceso en ejecución con mayor prioridad es el testeador, los procesos que utilizan mayor cantidad en memoria física son: Explorer con 10.796 KB; en memoria virtual tenemos: Internet Explorer con 174.912 KB, Explorer con 74.228 KB, EXCEL.EXE con 57.180 KB, tomando en cuenta estos valores podemos deducir que la memoria física y virtual asignada para cada proceso en este terminal es la adecuada y

además no existen procesos ajenos a los que se ejecutan normalmente. Para mayor información ver anexo 19 literal b.

SECRETARIA

En el terminal designado a secretaria es posible observar que los procesos que demandan de mayor memoria física son: Explorador de Windows con 2,168 KB, HP Photo & Imaging Gallery correspondiente al scanner con 5,512 KB, e Internet Explorer con 13,076 KB, en cuanto a memoria virtual se refiere los procesos con mayor memoria asignada son: Explorador de Windows con 12,932 KB, Monitor de dispositivos de imagen estática con 3, 300 KB; HP Photo & Imaging Gallery con 19,508 KB.

Internet Explorer con 21,598 KB; Microsoft Excel 15,028 KB; todos estos procesos tienen prioridad de ejecución normal. Por lo tanto se deduce que en este computador los procesos ejecutados se enmarcan dentro de lo normal en horas de trabajo por parte de la secretaria de Ocus. En detalle ver anexo 19 literal c.

CREDITO

En cuanto al computador designado a crédito podemos decir que los procesos que requieren mayor cantidad de memoria física son: Services con 19.800 KB, Norton Antivirus con 12,748 KB, Explorador de Windows con 17,648 KB los procesos que requieren de mayor memoria virtual son: Aplicación de servicios y controlador con 18,804 KB; Generic Host Process for Win32 Services con 107,104 KB Virus Definition Daemon con 16,424 KB; Internet Explorer 155,552

KB; mediante este análisis se ha podido llegar a la conclusión de que los procesos ejecutados en crédito son normales dentro del ámbito de trabajo, no se observa la presencia de procesos ajenos a las labores diarias. Para mayor información ver anexo 18 literal d.

CONTABILIDAD

En el computador asignado a contabilidad se observan algunos procesos entre los cuales están aquellos que requieren de mayor memoria física así: Norton Antivirus con 12,320 KB, Explorador de Windows con 21,068 KB, hpotdd01 (hp) 3,600 KB, Messenger con 3,912 KB; los procesos que requieren de mayor memoria virtual son: Aplicación de servicios y controlador con 18,312 KB, Internet Explorer con 174,852 KB Norton Antivirus con 85,184 KB; de lo que se puede deducir que en contabilidad los procesos están enmarcados dentro de la normalidad de las tareas propias de sus labores cotidianas. En mayor detalle ver anexo 18 literal e.

COMENTARIO:

En Proceses Pane o Panel de Procesos se muestra en detalle los procesos que se ejecutan en cada máquina, la memoria física y virtual que ocupan así como la prioridad de ejecución de todos los procesos; los procesos que se ejecutan en los equipos de Ocus, que tienen prioridad alta y que ocupan mayor cantidad de memoria física y virtual son Explorador de Windows, Internet Explorer, Impresoras, Inicio de sesión con Windows NT, etc. procesos que son necesarios

para el trabajo desempeñado por los empleados de la cooperativa Oscus; además se puede observar la ejecución Norton Antivirus.

Con lo mencionado anteriormente podemos deducir que en cada una de las máquinas se tiene la precaución de evitar el contagio de virus.

3.11.3.3 ANALISIS DE LOS RESULTADOS OBTENIDOS EN SYSTEM PANE

SYSTEM PANE – INFORMACIÓN GENERAL

Cajero Principal.- En el computador designado a cajero principal se puede observar que los 28 procesos en ejecución ocupan el 7.03% de CPU lo que quiere decir que el 92.97% tiene disponibilidad para ocuparlo en otras tareas; con estas cifras se deduce que los procesos que se ejecutan en este terminal no son pesados para el mismo; (ver anexo 20 literal a).

Otro dato importante es la capacidad de memoria física que tiene el computador siendo esta: 253.424 KB, la capacidad de memoria libre es: 112.088 KB; con lo que se deduce que se está ocupando un 141.416 KB; en cuanto a memoria virtual se tiene 477.800 KB; y usada 142.864, fue posible registrar un promedio de 50 archivos de lectura en KB/s y 1 archivo de escritura en KB/s de todos estos datos es posible pensar que en forma general el computador es apto para desempeñar las labores cotidianas del receptor pagador de Oscus.

Cajero Secundario.- En este computador se logró recopilar importante información como: porcentaje de CPU que ocupan los 29 procesos en ejecución, siendo este: 2.35% de lo que se deduce que el 97.65% se lo puede usar en otras tareas; estas cifras dejan ver que los procesos en ejecución no demandan mayor esfuerzo del mismo; (ver anexo 21 literal a)

La capacidad de memoria física que tiene el computador, con un total de 253.424 KB, 114.452 KB de memoria libre; entonces se está ocupando 138.972 KB de memoria física; en cuanto a memoria virtual se refiere 477.800 KB están libres; y usados 142.864 KB, además se registró un promedio de 3 archivos de lectura en KB/s y 1 archivo de escritura en KB/s de todos estos datos es posible pensar que en forma general el computador es apto para desempeñar las labores cotidianas del recibidor pagador de Oscus.

Secretaria.- En el momento del análisis con TaskInfo se recopiló valiosa información como: cantidad de procesos que se ejecutaron es así que arroja un resultado de 22 procesos, el 15.22% de CPU está en uso, mientras que el 84.74% esta disponible, en memoria física libre se tiene 31.088 KB y un total de 261.628 KB.

En memoria virtual 515.636 KB, y se utilizó 331.816 KB de memoria en la ejecución del sistema, procesos y aplicaciones, en forma general el computador designado a secretaria en comparación con los anteriores tiene deficiencias en cuanto a ejecución de procesos y el porcentaje de CPU que se requiere para ejecutarlos (Ver anexo 22 literal a).

Crédito.- En la oficina de crédito fue posible detectar en el momento del análisis la ejecución de 24 procesos, ocupando 3.91% de CPU, quedando así el 96.09% libre, además se determinó que el total de memoria física es 515.568 KB, con 323.336 KB de memoria física libre; en memoria virtual libre dispone de 1.115.480 KB. En procesos, ejecución del sistema y aplicaciones intervinieron 114.712 KB, además se registró un promedio de 61 archivos de lectura en KB/s y 10 archivos de escritura en KB/s. De estas cifras se puede deducir que en este computador no se presentan problemas que impidan el buen funcionamiento del mismo. (Ver anexo 23 literal a)

Contabilidad.- En este computador se logró recopilar información valiosa acerca del porcentaje de CPU que ocupan los 25 procesos en ejecución siendo este el 0.79%, mientras que el 99.21% restante se lo puede usar en otras tareas; con estas cifras se deduce que los procesos que se ejecutan en este terminal no demandan mayor esfuerzo del mismo; (ver anexo 24 literal a); 515.804 KB son la totalidad de memoria física, teniendo 351.296 KB de memoria libre; de modo que se está ocupando 164.272 KB; en cuanto a memoria virtual se refiere 1.108.284 KB están libres.

La cantidad de memoria virtual que intervino en aplicaciones, sistema fue de 151.804 KB, además se registró un promedio de 12 archivos de lectura sobre segundo /s y 12 archivo de escritura sobre segundo (/s) de todos estos datos es posible pensar que en forma general el computador es apto para desempeñar las labores cotidianas del contador.

SYSTEM PANE – INFORMACIÓN DEL CPU

Los datos que fueron posibles registrar en los computadores auditados son:

TABLA No 25: INFORMACION DEL CPU

DEPARTAMENTO	VENDEDOR DE CPU	TIPO DE CPU	FAMILIA, MODELO	RELOJ EN MHz
Cajero Principal	INTEL	Intel(R) Pentium(R) 4 CPU 2.80GHz	15 / 2 / 9 Original OEM processor	2.800
Cajero Secundario	INTEL	Intel(R) Pentium(R) 4 CPU 2.40GHz	15 / 2 / 7 Original OEM processor	2.391
Secretaria	INTEL	INTEL Pentium II	6 / 3 / 4 Original OEM processor	264
Crédito	INTEL	Intel(R) Pentium(R) 4 CPU 2.80GHz	15 / 2 / 9 Original OEM processor	2.799
Contabilidad	INTEL	Intel(R) Pentium(R) 4 CPU 2.80GHz	15 / 2 / 9 Original OEM processor	2.800

Autor: Silvana Monge

Fuente: Oscus Sucursal Latacunga

Con una simple inspección de los datos de la tabla anterior es claro darse cuenta que el computador designado a secretaria muestra bajas características en cuanto a CPU se refiere, con lo que podemos argumentar; que talvez este sea un catalizador importante para el anormal funcionamiento de las labores cotidianas en el mencionado departamento.

SYSTEM PANE – TODOS LOS ARCHIVOS ABIERTOS

Cajero Principal.- En el computador designado para las tareas de caja, mediante el análisis se pudo detectar la presencia de archivos comunes como: Menú Inicio, Impresoras, Windows, ayuda, tipos de letra, Windows NT, Internet Explorer, etc.(ver anexo literal 20 c) pero también fue posible observar archivos quizá innecesarios como lo son Windows Media Player y Pinball referentes a ejecución de archivos de audio, juegos, que por ningún motivo deberían ser ejecutados en una institución bancaria.

Cajero Secundario.- En lo referente al cajero secundario se logró detectar archivos como: Security, Windows NT, Internet Explorer, Outlook Express, Microsoft Excel Accesorios, Menú Inicio, etc. (ver anexo 21 literal c) además se observó la presencia de archivos de audio y juego como los son: Pinball, Mi música y Windows Media Player, archivos que normalmente no están abiertos en un área pública como lo es cajas.

Secretaria.- En secretaria se observa la presencia de archivos como: Archivos Temporales de Internet, Tipos de letras, Norton Antivirus, Explorer, Hp impresora, Scanner, archivos necesarios e indispensables para el desarrollo normal de las labores designadas a secretaria. (Ver anexo 22 literal c)

Crédito.- Gracias al análisis de TaskInfo se detectó en el terminal de crédito los siguientes archivos: Windows, Windows NT, Internet Explorer, Outlook Express, entre otros (ver anexo 23 literal c).

En este terminal también se observa la presencia de archivos de juego y música como: Pinball y Windows Media Player, la ejecución de estos últimos es muy poco usual en áreas que tienen contacto directo con el público.

Contabilidad.- En contabilidad se analizó el computador designado esta área y se logró encontrar archivos abiertos como: Outlook Express, Internet Explorer, Controladores, Tipos de letras, etc. (ver anexo 24 literal c) además se ejecutan en este terminal archivos que no son frecuentes en áreas de trabajo como son: Pinball y Windows Media Player.

SYSTEM PANE – TODAS LAS CONEXIONES

Cajero Principal.- En lo referente a las conexiones es posible visualizar que en el cajero principal se está utilizando protocolo TCP/IP, Udp; el puerto local permanece en estado de escucha, luego solicita conexión y permanece en estado de espera y finalmente establece conexión con el puerto remoto 180.180.20.13 que corresponde al cajero secundario, de estos datos es fácil deducir que entre cajero principal y secundario existe comunicación. (Ver anexo 20 literal d)

Cajero Secundario.- Al igual que en cajero principal se está utilizando protocolo TCP/IP, Udp; el puerto local permanece en estado de escucha, solicita conexión y la establece con los puertos remotos 180.180. 2. 42, 180.180.30.13, 180.180.20.12

este ultimo corresponde a cajero principal, con lo que se confirma la comunicación entre cajero principal y secundario. (Ver anexo 21 literal d)

Secretaria.- En secretaria el protocolo que se usa es igual al de cajas, el terminal de secretaria establece comunicaciones con los puertos remotos: 180.180.20.13 correspondiente a cajero secundario, SERVERLATACUNGA, SRVOSCUS, 180.180.30.30, 180.180.40.40, 180.180.50.50, AUDITORINTERNO

Con los datos anotados se deduce la buena comunicación entre todos los terminales de la gran red Oscus, poniendo así en claro el buen funcionamiento de la red. (Ver anexo 22 literal d)

Crédito.- En el área de crédito se está utilizando protocolo TCP/IP, Udp; el puerto local permanece en estado de escucha, luego solicita conexión posteriormente establece conexión con el puerto remoto 180.180.2.30, 180.180.2.42, 180.180.20.14 este último corresponde a gerencia, luego establece comunicación con los puertos remotos 180.180.30.13, 180.180.40.75. De estos datos es fácil deducir existe comunicación entre todos los terminales locales y remotos. (Ver anexo 23 literal d)

Contabilidad.- En contabilidad se ejecuta protocolo TCP/IP, Udp; al momento de la ejecución de TaskInfo 2003 contabilidad permanece en estado de escucha y espera sin establecer contacto con otro terminal, pero tal circunstancia es

aceptable puesto que no representa amenaza alguna para la sucursal. (Ver anexo 24 literal d)

SYSTEM PANE -- DRIVERS

En lo referente a drivers fue posible detectar que terminales como cajero principal, cajero secundario, contabilidad, crédito tienen los mismos drivers siendo estos: Sistema y núcleo de Windows NT, Controlador ACPI para NT, Enumerador PCI Plug and Play de NT, Controlador de disco con tolerancia a errores, Controlador de E/S del Administrador de discos de Windows NT, Controlador de filtro del sistema de archivos para Restaurar sistema, Controller Hub for Intel Graphics, Driver Video Port Driver, USB 1.1 & 2.0 Port Driver, Controlador de clase de teclado, Controlador de puerto paralelo, Controlador del dispositivo de serie, Serial Port Enumerator, Floppy Disk, Controller Driver, SCSI CD-ROM Driver, Controlador de filtros de sonido Redbook, SoundMAX Integrated Digital Audio, Controlador del dispositivo de procesador Peer-to-Peer Tunneling Protocol Parallel Technologies DirectParallel IO Library System Management BIOS Driver Intel Graphics Platform (SoftBIOS) Driver for Windows 2000(R) & Windows XP(TM), RAS Automatic Connection Driver.

TCP/IP Protocol Driver, NetBIOS interface driver, IP Network Address Translator, CD-ROM File System Driver, Controlador Win32 multiusuario, Controller Hub for Intel Graphics Driver, Controlador de puerto paralelo VDM.

TABLA No 26 SYSTEM PANE – INFORMACIÓN DEL SISTEMA

OPERATIVO

: SISTEMA OPERATIVO	CAJERO PRINCIPAL	CAJERO SECUNDARIO	SECRETARIA
Sistema Operativo	Windows XP	Windows XP	Windows 98 SE
Version	5.1	5.1	4.10
Build	2600 Service Pack 2	2600 Service Pack 2	2222 A
Tiempo ultimo de reinicio	4:47:17	3:30:38	5:55:19
Nombre del computador	2CAJA1	2CAJA2	2SECRETARIA
Windows Directory	C:\Windows	C:\Windows	C:\Windows
System Directory	C:\Windows\system32	C:\Windows\system32	C:\Windows\system32
Nombre del usuario	caja	caja	computo
Nombre del terminal	2Caja1	2Caja2	2secretaria
Nombre del terminal /dirección #0	2Caja1 : 180.180.20.12	2Caja2 : 180.180.20.13	2secretaria : 180.180.20.11
Estado del suministro de poder	Online	Online	Online
Estado de la batería	No system battery	No system battery	No system battery
Porcentaje de la batería	Desconocida	Desconocida	Desconocida
Tiempo estimado de vida de la batería	Desconocida	Desconocida	Desconocida
SISTEMA OPERATIVO	CONTABILIDAD	CREDITO	
Sistema Operativo	Windows XP	Windows XP	
Version	5.1	5.1	
Build	2600 Service Pack 1	2600 Service Pack 1	
Tiempo ultimo de reinicio	3:20:14	4:19:37	
Nombre del computador	2CONTABILIDAD	2ANALISTA	
Windows Directory	C:\Windows	C:\WINDOWS	
System Directory	C:\Windows\system32	C:\Windows\system32	
Nombre del usuario	contabilidad	analista	
Nombre del terminal	2contabilidad	2ANALISTA	
Nombre del terminal /Dirección #0	2contabilidad : 180.180.20.15	2ANALISTA : 180.180.20.16	
Estado del suministro de poder	Online	Online	
Estado de la batería	No system battery	No system battery	
Porcentaje de la batería	Desconocida	Desconocida	
Tiempo estimado de vida de la batería	Desconocida	Desconocida	

Autor: Silvana Monge
Fuente: Oscus Sucursal Latacunga

3.11.3.4 ANALISIS DE LA RED IMPLEMENTADA EN OSCUS

Para analizar la red se utilizaron monitores de red como: Ethereal, Ntwork Inspector, Network Diagram, acompañado de Visio 2003, y PRTG para anchos de banda, con la instalación de estos se logró obtener el siguiente análisis:

La red implementada en OSCUS es una red pública, se llega a esta definición puesto que después de obtener resultados al instalar Network inspector; (anexo número 27) en el que se observa que el ip de la red 180. 180. 002. 009 en los que los dos primeros octetos determinan el tipo de red en este caso de tipo B como lo muestra la siguiente tabla:

TABLA No 27 CLASES DE IP

CLASES DE IP	RANGOS DE IP
A	1 - 126
B	128 - 191
C	192 -223
D	224 – 239
E	240 - 255

Fuente: Manual de Redes
Autor: Universidad Técnica de Ambato

También nos indica el octeto 180. que se trata de una red pública, además según RFC 1918 (Request For Connects) las Ip. Privadas no pueden conectarse a Internet, y todo el sistema de Oscus funciona en un ambiente Internet.

Para la evaluación de la red se instaló el software denominado Network diagram, con el objetivo de graficar la red, en vicio y como lo muestra el anexo número 29 en el switch utilizado para la comunicación está desactivado el protocolo SNMP, impidiendo graficar en un 100% el esquema físico de la red, de lo que se deduce la buena seguridad en la red por parte del administrador, evitando así el acceso de hackers informáticos que puedan sabotear la red.

Otro software instalado para este análisis es Ethereal con el que se confirma la tesis de que la red es plana, por la detención de broadcast en gran número, solicitando la actualización de ARP y protocolo NBS como se ve en el anexo número 28, en promedio el tiempo de retardo de recepción de datos es 0.4783737 segundos y se envían frames de 60 bytes en un promedio de 0.5052626 segundos.

En los porcentajes capturados por Ethereal se observa que el protocolo ARP es el que muestra mayor porcentaje aseverando la presencia de broadcast.

En circunstancias normales la información de entrada es mayor que la de salida esto se debe a la constante actualización de la sucursal Latacunga a la matriz.

Como se muestra en el anexo número 28 el flujo de la información varía al momento de acceder a Internet, haciendo que la curva de ingreso de información supere a la de salida

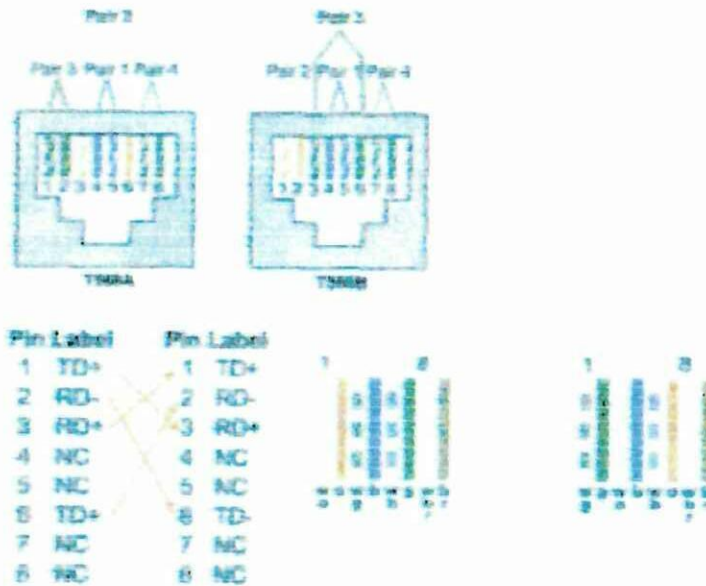
Oscus tiene contratado un ancho de banda de 11 megabits por segundo, dividido en 6 megabits para recepción y 5 megabits para transmisión.

Cada usuario utiliza un promedio de 41.436 Kbytes por intervalo de 60 minutos.

En cuanto al estado físico del cableado para el funcionamiento de la red se puede decir que se observa mantenimiento, se constató buen estado los conectores cableado, también fue posible observar el cuidado en el tendido del cable es decir el uso de canaletas, pinzas, seguros, contribuyendo la seguridad y estética del cableado.

Los conectores utilizados son rj 45, cable UTP categoría 5, con tecnología par trenzado de acuerdo al código de colores como lo muestra la siguiente figura:

Fig. 3.1 CÓDIGO DE COLORES.



Otra de las actividades planteadas en esta fase es el desarrollo de hojas de hallazgos como se muestra a continuación

3.12 CARTA DE INTRODUCCION

Una vez analizada toda la información obtenida al desarrollar cada una de las tareas el siguiente paso es redactar una carta de introducción dirigida al gerente de OSCUS Sucursal Latacunga, la cual tiene la característica de ser presentada únicamente al gerente de la institución, en tanto que el Informe Final de Auditoría, puede tener tantas copias como sean necesarias. Para mayores detalles la carta de introducción se presenta en el anexo dentro del CD de apoyo.

3.13 INFORME FINAL DE AUDITORÍA



UNIVERSIDAD TECNICA DE COTOPAXI
COOPERATIVA DE AHORRO Y CRÉDITO OSCUS



INFORME FINAL DE AUDITORÍA

AUDITORIA INFORMÁTICA EXTERNA A OSCUS SUCURSAL
LATACUNGA

INFORMACIÓN INTRODUCTORIA

TIPO DE AUDITORIA:	Externa.
INSTITUCIÓN AUDITADA:	Cooperativa de Ahorro y Crédito Oscus Sucursal Latacunga
INICIO DE AUDITORÍA:	26/06/04
REDACION DE INFORME FINAL:	17/06/05
AUDITOR:	Silvana Monge
DIRECTOR RESPONSABLE:	Ing. Emma Campaña Riofrío.

PERSONAL AFIN: Para la realización de la investigación se encuestó a los usuarios del sistema, a los socios de Oscus y entrevistó al Ing. Marco Hidalgo en

calidad de Gerente de Sucursal, al Ing. Carlos Santamaría Jefe del Área de Informática, Ing. Juan Freire Analista/Programador, Ing. Francisco Lozada Administrador.

MOTIVO DE LA AUDITORIA

La Auditoria Informática externa a Oscus sucursal Latacunga se llevó a efecto ante la necesidad de este servicio, puesto que no se había realizado tal evaluación a nivel informático, otra razón importante y de peso es el aporte que esta investigación brinda a la institución como trabajo investigativo para el mejoramiento del control del recurso informático que posee Oscus, además este trabajo puede ser tomado como base para futuras investigaciones.

La idea de ejecutar una Auditoria Informática surge ante el contacto directo que tuvo el investigador al realizar una pasantía de aproximadamente 4 meses, en la que pudo palpar la realidad del establecimiento, sin afán de en estas palabras expresar mala imagen o situación de Oscus simplemente la ausencia de auditoría informática en esta sucursal.

OBJETIVOS DE LA AURITORIA

5.1.- OBJETIVO GENERAL:

- Desarrollar una Auditoría Informática en la Cooperativa de Ahorro y Crédito “OSCUS” Ltda. Sucursal Latacunga para determinar el adecuado uso de los recursos informáticos mediante la aplicación de técnicas y herramientas apropiadas, para obtener resultados consistentes que ayuden al mejoramiento del aprovechamiento de los recursos informáticos que dispone la institución.

5.2.- OBJETIVOS ESPECÍFICOS:

- Diagnosticar el estado informático en la Cooperativa de Ahorro y Crédito “OSCUS” Ltda. Sucursal Latacunga, mediante la aplicación de auditoría informática para el mejoramiento de la institución
- Determinar la compatibilidad de funcionamiento simultaneo del Sistema Operativo y el Software de base con todos los subsistemas existentes, así como la compatibilidad del Hardware y del Software instalados, mediante pruebas para comprobar su buen funcionamiento
- Auscultar la observancia de las normas teóricamente existentes en el departamento de Informática y su coherencia con las del resto de la

empresa, aplicando la observación para poder aportar con orientaciones adecuadas.

- Determinar la existencia de Procedimientos Generales Informáticos, a través del estudio de documentación para dar un criterio pertinente.
- Verificar la existencia de seguridades para evitar robos y la utilización de copias piratas.
- Analizar el buen funcionamiento de las comunicaciones y de la red con la central ubicada en Ambato. Mediante la participación directa para poder emitir una buena evaluación.
- Auscultar la concordancia de los cargos además de la capacitación y entrenamiento que reciben los empleados de OSCUS, a través de la observación directa para emanar sugerencias acertadas.
- Ejecutar la Auditoría Informática en la Cooperativa de Ahorro y Crédito OSCUS Ltda. Sucursal Latacunga mediante la aplicación de métodos y técnicas adecuadas para mejorar el funcionamiento informático de la institución.

ALCANCE DE LA AUDITORÍA

Esta Auditoría Informática cubrió el período comprendido entre el 26/06/04 y la presente fecha y se examinaron, entre otros, los siguientes aspectos: Sistema: seguridades lógicas, uso y actualización de claves, operatividad del sistema, estudio de factibilidad, aplicación y cumplimiento de políticas, normas para

diseño, desarrollo e implementación del sistema, idoneidad del personal informático, observancia de normas, existencia de procedimientos generales, funcionamiento de las comunicaciones, concordancia en los cargos, etc. Se evitará tocar temas como movimientos financieros, adquisiciones, administración de usuarios, datos privados de gerencia y contabilidad.

En el anteproyecto se dividió a los recursos informáticos en cuatro grandes grupos de los cuales de acuerdo al transcurso de la investigación se ha ido desglosando en tópicos específicos que ayuden a obtener conclusiones veraces y recomendaciones acertadas. Así:

EVALUACION DE LA SUCURSAL LATACUNGA:

- Ubicación geográfica.
- Cumplimiento de seguridades físicas
- Ubicación de equipos
- Organización de salas de trabajo
- Uso de jerarquías
- Determinación de funciones
- Seguridad física de los equipos
- Origen de los equipos
- Ambiente de trabajo

EVALUACIÓN DEL AREA DE SISTEMAS

- **Diseño y programación de sistemas**
 - Uso de normas de programación
 - Aplicación de políticas del Área de Informática
- **Datos fuente y cifras de control**
 - Cumplimiento de políticas de seguridad
 - Cumplimiento de políticas de uso de password
 - Cumplimiento de políticas de obtención de respaldos
- **Controles de salida de información**
 - Cumplimiento de políticas de respaldo y liberación de datos
 - Obtención de respaldos
 - Frecuencia de obtención de respaldos
- **Controles de medios de almacenamiento masivo**
 - Cumplimiento de políticas de acceso al área de procesamiento de datos.
 - Observancia de seguridades físicas
 - Control de acceso a personal autorizado
 - Existencia de alarmas de humo, fuego, extintores
 - Control de temperatura iluminación y ventilación en área de servidores.
 - Existencia de advertencia para el uso de equipos y comportamiento en el área especialmente de archivo y servidores.

- Cumplimiento de políticas para etiquetado y tratamiento de cintas magnéticas y backups.
- Orden, designación de utensillos de oficina y papelería.
- Medidas de seguridad para el acopio de backups.
- Evaluación de seguridad lógica y confidencial.
 - Evaluación de plan de contingencias
- Reportes generados por el sistema
 - Necesidad
 - Datos generados
 - Veracidad de datos
- Evaluación de la Base de Datos
 - Plataforma
 - Normalización
 - Tamaño
 - Documentación
 - Formas de conexión con el Frond End
- Evaluación del código fuente
 - Lenguaje de programación
 - Operatividad
 - Susceptibilidad del código
 - Integración
 - Modularidad
 - Lógica de programación

- Evaluación del manual de usuario
 - Existencia
 - Facilidad de uso
 - Presentación
 - Detalle
 - Difusión
- Evaluación de las aplicaciones del sistema
 - Funcionalidad
 - Facilidad de uso
 - Funcionamiento
 - Necesidad
 - Satisfacción del usuario

EVALUACIÓN DE RECURSO HUMANO

- Número de puestos de trabajo
- Número de empleados por puesto de trabajo
- Coherencia de cargos
- Curriculums
- Capacitación informática
- Puestos de trabajo en el Área de Informática
- Número de empleados por puestos de trabajo

EVALUACION DE HARDWARE Y SOFTWARE

SOFTWARE:

- Existencia de un inventario software
- Licencias de uso
- Sistema Operativo de las máquinas
- Programas instalados en las máquinas
- Archivos de mayor uso
- Determinación de archivos no autorizados

HARDWARE:

- Existencia de un inventario hardware
- Estado de los equipos
- Características de CPU (Central United of Procesing/Unidad Central de Procesos)
- Observancia de políticas de uso de equipos

EVALUACION DE LA RED IMPLEMENTADA EN OSCUS

- Estado del cableado
- Tipo de cableado
- Tipo de conectores
- Tipo de tecnología o código de colores
- Flujos de entrada salida de información

- Tiempos de transacción de frames o paquetes de trabajo.
- Anchos de banda.

BASE LEGAL

- Código de Trabajo
- Ley de contratación Pública
- Boletín de Auditoría Informática (facilitado por la Contraloría General del Estado Latacunga)
- Políticas del Área de Informática.
- Normas ISO 9000:2000
- Normas ISO SPICE
- Normas ISO 9001

INTRODUCCIÓN

Al ejecutar Auditoría Informática el principal objetivo es examinar, los procesos automáticos y aún los no automáticos relacionados; a fin de obtener una evaluación global de todos los aspectos que intervienen en el quehacer informático, cuando una institución decide realizar auditorías sean esta informáticas o no, está avanzando un paso delante de los acontecimientos, es decir ratificando los procedimientos bien ejecutados, y detectando a tiempo los pequeños errores que a la postre podrían convertirse en serias amenazas que

atenten en contra del buen funcionamiento de la institución; es por ello que luego del análisis de Oscus Sucursal Latacunga se obtuvieron los resultados positivos y negativos que requieren de atención para su mejoramiento, es así que en el aspecto de aciertos de Oscus se obtuvo:

EVALUACIÓN DE LA SUCURSAL LATACUNGA:

Debido a la ubicación geográfica de la Sucursal Latacunga, se puede decir que su edificación es segura, puesto que se halla fuera del alcance de ríos en caso de desbordamiento, no se encuentra en una zona forestal en la que se pueda provocar incendios, de lo que se deduce que geográficamente la sucursal se encuentra favorablemente ubicada tanto a nivel comercial como de seguridad, para mayores detalles se ilustra un croquis en el anexo No 3 contenido en el CD de apoyo.

En el edificio, las autoridades han tomado como medidas de seguridad la contratación de un guardia de vigilancia, cámaras de video, alarmas ubicadas en sitios estratégicos para que el personal pueda activarlas en caso de robo o asalto, estas alarmas están conectadas a la central de policía, de modo que se reciba auxilio inmediato, en las ventanas se han colocado barras protectoras, las puertas de ingreso a la institución cuentan con chapas, claramente se puede percibir seguridad física en la sucursal Latacunga.

Las salas de trabajo están organizadas funcionalmente, tomando en cuenta la comodidad del cliente es así que las áreas de mayor acceso al público están ubicadas en el primer piso, siendo estas: gerencia, secretaria y cajas, creando un agradable ambiente de trabajo.

La institución está organizada estructuralmente, definiendo jerarquías y estableciendo funciones, como se muestra en el anexo No 5.

Cabe aclarar que la sucursal está íntimamente ligada al área de informática, que funciona en la matriz la cual se encuentra ubicada en la provincia de Tungurahua, en la ciudad de Ambato, al igual que la sucursal este edificio se encuentra situado en un lugar seguro para mayores detalles se presenta un croquis en el anexo No 7.

Las políticas de seguridad en cuanto al acceso al área de informática se cumple a cabalidad, debido a que se requiere autorización para visitar las instalaciones de este departamento el cual se encuentra organizado en salas de trabajo siendo estas: recepción, desarrollo, servidores, archivo; también a nivel de estructural, jerárquico y funcional el área está organizada, como se muestra en el anexo No 8.

EVALUACION DEL SISTEMA

El sistema que emplea Oscus está creado internamente; el personal del área informática como primer paso efectuó un estudio de factibilidad en el que se ponen de manifiesto el análisis costo/beneficio, los recursos hardware y software necesarios, etc. Para el diseño del sistema se emplearon normas de diseño y programación de sistemas, de modo que el diseño fue guiado, más no una ejecución sin bases.

Dentro del área informática se han establecido políticas internas, que regulan el funcionamiento de la misma, estas políticas también se aplican al sistema como por ejemplo las políticas de obtención de respaldos, es así que en cumplimiento de ésta se obtienen respaldos diarios a inicio y fin de actividades, además mensuales, cada uno de estos backups son etiquetados cumpliendo con políticas de etiquetado, así también se cumplen políticas de seguridad y transferencia de cintas magnéticas, al trasladarlas del archivo del área de informática a una bóveda de un banco que cuenta con las medidas de seguridad necesarias para salvaguardar la información de Oscus.

Para asegurar el buen estado físico de las máquinas, del personal, de los medios de almacenamiento masivo, se cumplen políticas de acceso restringido de personal autorizado, se controla la iluminación es decir la incidencia directa de la luz solar ubicando a las maquinas fuera del alcance de los rayos solares, es decir lejos de

ventanales, especialmente el área de servidores, en donde se controla temperatura, tención eléctrica, ventilación, mediante la distribución de salas se obtiene una buena organización física del área de informática separando los materiales de escritorio o de fácil ignición de áreas sensibles como la de producción, además para contrarrestar posibles incendios, existen alarmas detectores de humo y fuego, extintores.

Otra medida de seguridad del equipo es la restricción de uso de los computadores, instalación de software denominado pirata, obtención de copias de información confidencial, uso de software únicamente con licencia, etc.

Una buena medida de precaución que posee el área de informática es el diseño y desarrollo de un plan de contingencias en el que se observan circunstancias como: fallo de equipos, ausencia de personal, sabotajes, robos, incursión de hackers, fallo eléctrico, paros u huelgas del personal, desastres naturales, cada uno de estos puntos contempla actividades antes, durante y después del desastre con la evaluación de daños, además establece grupos de acción, responsables, equipos que funcionarían como alternativa, lugares estratégicos que servirían de campo de operación paralela o sustituta.

En el sistema empleado en Oscus, se observa la seguridad lógica empleando claves de acceso y estableciendo niveles de accesibilidad es decir que no todos los usuarios pueden ingresar a todas las aplicaciones incluso dentro de los creadores del sistema existe jerarquías de acceso en este caso el administrador del sistema es

quien tiene la patria potestad de ingresar a todas las aplicaciones del sistema, a la codificación, a las Bases de Datos, a las tablas, etc. en cuanto las claves éstas tienen un rango de actualización de tres días, tiempo en el cual el sistema automáticamente solicita cambio de clave, también existe la opción de modificarla cuando el usuario sospeche que alguien logró descifrar su clave. El sistema genera reportes que son documentos necesarios especialmente para contabilidad, como por ejemplo, arqueos de caja, amortizaciones, encajes, etc.

La Base de datos fue creada en SQL Server, de Microsoft, el lenguaje de programación que utilizaron fue el C# Sharp orientado a Internet, trabajando en un ambiente Web, con herramientas Internet y el enlace usado es .NET .

Las plataformas utilizadas son de actualidad, sobre todo en la elección de las mismas se ha tomado muy en cuenta los requerimientos del usuario y las herramientas que más se ajustaron a las demandas tanto de programadores como de usuarios finales, fueron escogidas.

Todo el código de programación muestra funcionalidad, sintaxis correcta, utilización de clases.

Después del análisis de los recursos informáticos de los temas antes mencionados se presenta a continuación las falencias que representan mayor riesgo para la

Cooperativa Oscus Sucursal Latacunga, así como también las sugerencias para mejorar el control y aprovechamiento de los recursos informáticos. Así:

HECHO ENCONTRADO: DESCONOCIMIENTO DEL MANUAL DE USUARIO

El manual de usuario fue diseñado y creado por los autores del sistema que en este caso son los empleados informáticos del Área de sistemas Informáticos de la Matriz, pero al aplicar la técnica de verificación verbal a los empleados de la sucursal Latacunga el desconocimiento del mismo es inminente, para la contraparte también se indagó sobre este tema al jefe de Área Informática, quien supo manifestar la existencia pero no difusión de dicho documento. Analizando el manual de usuario se logró determinar que está dividido por módulos es de fácil uso, tiene un ambiente gráfico que le permite al lector comparar pantallas de aplicaciones con su computador, y ejecutar adecuadamente cada proceso dentro de su ámbito de trabajo.

CONSECUENCIAS: Ante tal desconocimiento los empleados de Oscus corren el riesgo de cometer errores en el manejo del sistema, enfrentar dificultades de operación del sistema, otra consecuencia del desconocimiento del manual de usuario es la inoperatividad del sistema por cuanto los operadores no pueden reaccionar con prontitud, causando demoras innecesarias. Al no distribuir el

manual de usuario se esta incumpliendo con la política Entrenamiento de la implementación y/o modificaciones del aplicativo, y desatendiendo al inciso número 400 – 03, del Boletín jurídico No 6 de la Contraloría General del Estado, con título: operación y mantenimiento que reza: “Para los sistemas incorporados a su gestión, en cada entidad se elaborarán procedimientos formales y detallados del funcionamiento y operación, tanto a nivel de usuarios como de la unidad de sistemas de información computarizados”

REPERCUCIONES: La inoperatividad del sistema puede repercutir en la imagen de la institución causando también malestar a nivel de usuarios finales o socios de Oscus.

CONCLUSIÓN

Los usuarios del sistema no tienen conocimiento sobre manual un manual de usuario.

RECOMENDACIÓN No 1

Una vez concluido con el desarrollo del Manual de usuario, éste debe ser aprobado por los funcionarios pertinentes, y dar pleno conocimiento del mismo a todos los usuarios del sistema empleado en Oscus. De este modo el empleado contará con el conocimiento suficiente para operar el sistema, recordando que una imagen vale más que mil palabras, un escrito es de gran ayuda a parte de la

capacitación o entrenamiento que se el puede dar al empleado especialmente a aquellos que ingresan a laborar en Oscus.

HECHO ENCONTRADO: FALTA DE CAPACITACIÓN INFORMÁTICA DEL PERSONAL

De acuerdo con las encuestas aplicadas a los empleados que manejan el sistema de Oscus Sucursal Latacunga del 100% de los encuestados se ha podido observar que un 71.42% manifiesta que considera deficiente la capacitación informática y de la revisión de el según Plan Operativo Anual del 2005 del Área Informática en el que se observó la existencia de una actividad que le permitiera al empleado de sucursales capacitarse a nivel informático; fue posible descubrir que el personal que tiene contacto directo con el sistema, por lo tanto con computadores no está suficientemente capacitado en uso de paquetes o solución de problemas sean estos en software o hardware, por lo tanto se está incumpliendo las políticas de Política de entrenamiento para el entrenamiento y/o modificaciones del aplicativo y capacitación del personal informático y afines. es un derecho del empleado recibir capacitación y entrenamiento por parte del empleador; de acuerdo con la Norma 400 – 10 con título Utilización de los Equipos, Programas e Información Institucional, numeral 2, en el que reza “La capacitación de funcionarios en la utilización de los equipos y programas”

CONSECUENCIAS: Los empleados que operan el sistema deben poseer conocimiento informático suficiente sobre manejo de hardware y software, capacidad de reconocimiento de las partes de su computador, etc., de modo que sea idóneo para solucionar en corto tiempo pequeños problemas sin tener que recurrir a los técnicos de mantenimiento, el desconocimiento informático puede acarrear consecuencias de inoperatividad o errores humanos en el sistema.

REPERCUSSIONES: Cuando en una institución las computadoras son el instrumento principal de trabajo, especialmente en este mundo de automatización, representa un grave error no estar actualizado en conocimientos informáticos, o capacitados para reparar pequeñas fallas del equipo que asemejan grandes problemas, que pueden repercutir en el tiempo óptimo de respuesta al cliente, creando malestar e insatisfacción.

CONCLUSIÓN

El conocimiento informático de los usuarios del sistema no es suficiente

RECOMENDACIÓN No 2

Con entrenamiento a nivel medio de: uso de paquetes, uso del sistema actual, mantenimiento de los equipos, el usuario del sistema estará en capacidad de responder con eficiencia a los requerimientos del socio, y a posibles inconvenientes con su equipo, lo que evitará recurrir al técnico de mantenimiento en consecuencia se disminuirá egresos, y tiempo inoperativo de los equipos.

HECHO ENCONTRADO: FALTA DE ENERGÍA ALTERNATIVA

Durante las visitas periódicas del investigador, en una de ellas, se pudo presenciar la falta de energía eléctrica en la ciudad de Latacunga por causa del mal clima, razón por la cual se suspendió el suministro de energía en la Sucursal Latacunga; apagándose de este modo los computadores de la misma, sin previo aviso ni la ventaja de un proveedor de energía adicional como lo es el UPS, generándose así inconvenientes en las transacciones y operaciones de archivos inconclusas o no guardadas, al momento del apagón. Falla por demás peligrosa para la buena imagen de la institución; puesto que los socios de la sucursal se vieron afectados debido a la incomodidad que causó alrededor de los 45 minutos que duró la interrupción. Por lo tanto se está incumpliendo la política de seguridad física del personal y los equipos.

CONSECUENCIAS: Una institución previsiva, debe contar con una alternativa en caso de fallo eléctrico, en caso contrario podrían desencadenarse consecuencias como, pérdida de información, retraso en la ejecución de las labores diarias, y sobre todo puede acarrear consecuencias de mala imagen, o desconfianza en el socio.

REPERCUCIONES: un apagón especialmente en una institución bancaria, repercute principalmente y como el más afectado en la programación de

actividades del día del socio, puesto que es a este personaje a quien se le afecta por no poder servirle en las necesidades que solicita.

CONCLUSIÓN

En la cooperativa de ahorro y crédito Oscus Sucursal Latacunga existe falencias con respecto a la prevención de interrupciones eléctricas.

RECOMENDACIÓN No 3

En toda institución más aún en una de carácter bancario, se debe prever una situación de falla eléctrica y dotar de una alternativa para seguir funcionando mientras se soluciona el problema principal, por lo que se recomienda a las autoridades pertinentes tomar cartas en el asunto y facilitar a la sucursal de una fuente de energía adicional que subsane un inconveniente tan común y desastroso como es el corte de energía eléctrica.

HECHO ENCONTRADO: FALTA DE SEGURIDAD FÍSICA EN EL SERVIDOR DE LA INSTITUCIÓN

De la observación de campo y el reconocimiento físico mediante la visita previa a Oscus, aplicando técnicas de observación directa fue posible determinar que en la sucursal Latacunga se ha destinado al servidor al área de cajas si bien es cierto, posee restricción de acceso a los socios a la mencionada, y el servidor cuenta con seguridad lógica, no se debe desestimar posibles accidentes o intentos de dañar

físicamente al servidor, puesto que dada la importancia de este requiere de cuidado, es decir se está faltando a la política de seguridad física del personal y equipos.

CONSECUENCIAS: Si el servidor falla la consecuencia inmediata es la inoperatividad de los equipos, produciendo malestar hasta la compostura del mismo.

REPERCUCIONES: Como en los anteriores hallazgos el principal afectado es el socio, causando que éste cree inseguridad, desconfianza y comentarios desfavorables para la institución.

CONCLUSIÓN

En Oscus Sucursal Latacunga existe inseguridad física para el servidor, pese a la importancia de este terminal.

RECOMENDACIÓN No 4

Debido a que este terminal es muy importante para el funcionamiento de la institución se recomienda colocar una mampara o armario con seguro o chapa para resguardar de cualquier intento por dañar al equipo y además protegerlo de las condiciones ambientales como el polvo o humedad.

HECHO ENCONTRADO: EQUIPOS DESACTUALIZADOS

De la observación documental del inventario de los equipos existentes en Oscus, de la constatación física de los equipos de Oscus en la observación de campo y de los resultados que arroja el software instalado en cada terminal (TaskInfo) se pudo observar que los equipos designados a secretaria, gerencia y un terminal de crédito están desactualizados, así como la impresora destinada a cajas que además de estar obsoleta no funciona adecuadamente, debido a la carga de trabajo especialmente en secretaria se hace indispensable un computador de mejores características, este fallo se debe principalmente a la poca planificación en la adquisición de los equipos y a la incomunicación de los responsables directos con los usuarios para conocer, las necesidades que tienen estos. Además no se pudo conocer un análisis FODA de recurso humano, hardware y software en la Sucursal Latacunga como lo exige en el numeral 400 - 02 del Boletín Jurídico N6 de la Contraloría General del Estado inciso 1 que reza: “El Plan Integral debe contener lo siguiente: 1. Fase organizacional referente a la misión de la entidad, estructura orgánica, ANÁLISIS FODA situación actual del área informática en: recursos humanos, HARDWARE y SOFTWARE”.

Para la actualización o adquisición de equipos la ley exige se estructure un Plan Integral Informático, así el numeral 400 – 02 con título: “plan informático, adquisición o actualización de sistemas” reza: “Los sistemas de información computarizados se generan de acuerdo a los requerimientos o necesidades

establecidas en cada entidad del sector público, y será necesario que la máxima autoridad apruebe un **PLAN INTEGRAL INFORMÁTICO**, con sujeción a las disposiciones vigentes. Dicho plan será de carácter obligatorio, independiente del nivel de complejidad o tamaño de la entidad, además será el que regule y determine el desarrollo informático de la institución a corto y mediano plazo.”, en este caso no existe una política que regule la adquisición de los equipos o el requerimiento de actualización dependiendo del trabajo y las necesidades del empleado.

CONSECUENCIA: La principal consecuencia de poseer un equipo desactualizado es el incremento de tiempo en la ejecución de las tareas.

REPERCUCIÓN: Este fallo repercute principalmente en la explotación de las capacidades físicas, mentales de los empleados, el operador del computador puede ser un excelente empleado pero si sus aptitudes se ven limitadas por no poseer un equipo adecuado, no podrá cumplir satisfactoriamente con sus tareas.

CONCLUSIÓN

En la cooperativa de ahorro y crédito Oscus Ltda. Sucursal Latacunga existe desactualización de equipos de computo en al menos el 30% de los terminales disponibles en la institución.

RECOMENDACIÓN No 5

Para lograr un buen funcionamiento de los equipos se recomienda reemplazarlos por unos más actualizados, como ya se lo a realizado en otros departamentos (Ej. cajas), de este modo se obtendrá mejores resultados en la operatividad de los equipos, como en satisfacción de los usuarios informáticos, socios de Oscus contribuyendo así al incremento de la eficiencia y eficacia del servicio cooperativo y además con instrumentos de punta disponibles para el trabajo, se podrá conseguir mejorar la imagen de la institución a nivel de los socios, de otras instituciones, con lo que será posible atraer a las personas que aún no forman parte de la gran familia Oscus e incrementar el movimiento financiero dentro de la sucursal.

HECHO ENCONTRADO: MAL USO DE LOS EQUIPOS

En la observación de campo mediante la utilización de software de análisis como lo es TaskInfo fue posible descubrir la utilización de software no autorizado en ninguna institución más aún al tratarse de una institución financiera, TaskInfo detectó archivos abiertos de audio como es MediaPlayer, y de juego como Pinball, dichos archivos no deberían haber sido abiertos, ni ejecutados por parte de los empleados de Oscus ni en horas laborables ni en las de aparente ocio. Se debe tener extremo cuidado en el uso del recurso informático puesto que la instalación de juegos representa un grave riesgo para la información contenida en el

computador puesto que esta puede ser infectada con algún tipo de virus acarreado por los juegos, esto se debe a la falta de monitoreo del uso del recurso informático por parte de los responsables directos. Violando así la política de uso y acceso restringido a equipos; también en el numeral 400 – 10 del Boletín Jurídico No 6 de la Contraloría General del Estado con título: utilización de los equipos, programas e información institucional reza: “Los equipos y programas serán utilizados exclusivamente en las actividades propias de la institución.”

CONSECUENCIA: Una grave consecuencia que puede producirse por el mal uso de los equipos es introducir un virus informático, presente en discos piratas, de video o juegos.

REPERCUCION: al utilizar indebidamente el equipo se puede repercutir en la comodidad del cliente al causar molestia con la ejecución de archivos de audio, o interrumpir el buen funcionamiento del sistema con la ejecución de software pirata especialmente de juegos.

CONCLUSIÓN

En los terminales de la cooperativa Oscus Sucursal Latacunga existe la presencia de archivos de audio y entretenimiento.

RECOMENDACIÓN No 6

Con el afán de obtener mayores y mejores resultados en el desempeño diario de los empleados de Oscus se recomienda eliminar los archivos de juego, de música, y de video, además es recomendable monitorear el uso de las terminales, como se manifiesta en el Boletín Jurídico No 6 numeral 400 – 10 en el que dice: “La máxima autoridad de cada entidad pública o por su delegación los directivos y jefes de las unidades administrativas, establecerán procedimientos para asegurar el uso eficiente, eficaz y económico de los equipos, programas de computación e información computarizada, a través de: 1. El registro y seguimiento de la operación de los mismos;”

CAPITULO VI

CONCLUSIONES
RECOMENDACIONES

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

Para redactar las conclusiones de la investigación, se ha tomado muy en cuenta los resultados obtenidos en las encuestas a los usuarios del sistema, a los socios de Oscus, entrevistas a los técnicos del Área de Sistemas Informáticos, la opinión personal del investigador generada en la observación de campo, en la observación documental del investigador, en la experiencia personal del investigador, el desarrollo mismo de Auditoría Informática etc. Así:

- En lo que se refiere a capacitación del personal de Oscus a nivel informático, se concluye que es insuficiente, conclusión que se ve fundamentada en las respuestas de los usuarios del sistema encuestados, en la observación directa, y de la observación documental del plan anual de actividades del área de informática.

- Se concluye que si el usuario del sistema se siente insatisfecho con los resultados del Área de Sistemas Informáticos, entonces nos estamos enfrentando a la poca o nula comunicación entre los técnicos de la matriz y los usuarios de la sucursal Latacunga.

- Después de indagar entre los empleados de Oscus, se llegó a la conclusión de que los mismos no tienen conocimiento sobre un plan de contingencia que les guíe ante la presencia de posibles desastres.

- Al ejecutar observación documental se concluyó que los usuarios del sistema no poseen un manual de usuario que les permita, guiarse en el manejo del sistema.

- Después de la presencia de la falta de energía eléctrica en la sucursal, durante un apagón en la ciudad de Latacunga el día miércoles, 8 de diciembre del 2004 aproximadamente a las 16:00, se concluye que en la Cooperativa Oscus no existe la prevención de cortes de energía eléctrica.

- Después de acopiar los resultados obtenidos por el software instalado en las máquinas (TaskInfo) para monitorear el uso de los mismos, se determinó que en ciertos terminales están instalados archivos de juego y audio.

- Los computadores de la sucursal Latacunga son medianamente actualizados en consecuencia no puede existir subutilización de equipos.

- Al investigar sobre las capacidades de los técnicos de la matriz se puede concluir que los mismos están aptos para desarrollar software interno.
- Luego de la observación directa se llega a la conclusión de que la operatividad del software es buena, con un buen sistema operativo, y adecuada seguridad lógica.
- Se concluye que los datos, archivos físicos y lógicos, y toda la información de Ocus, están correctamente organizados.

4.2 RECOMENDACIONES:

- En lo referente a la capacitación de los empleados de Ocus es recomendable, otorgar cursos de informática a nivel, de igual manera es recomendable entrenarlos en el manejo de extintores, técnicas de venta y atención al cliente.
- Se recomienda a los técnicos de la Matriz comunicarse más a menudo con los usuarios finales del sistema que desarrollen, mediante la aplicación de charlas y entrevistas; debido a que los sistemas que se diseñen e implanten tienen por objetivo cubrir las necesidades del usuario y si nos olvidamos de dialogar con los usuarios a quienes va dirigido el sistema; se estaría corriendo el riesgo de omitir quizá requerimientos esenciales para el usuario final.

- Puesto que el personal de toda institución requiere del conocimiento de un plan de contingencia para poder actuar con serenidad y seguridad ante desafortunados desastres, por lo que se recomienda facilitar el plan de contingencia existente y efectuar ciertas adaptaciones en el mismo para la sucursal Latacunga
- Es recomendable dotar a los usuarios del sistema de un manual de usuario, no es suficiente una charla, sobre el funcionamiento del sistema, el empleado debe contar con un documento que lo ayude a recordar, tampoco es suficiente desarrollar el manual, si no se va a verificar que el personal lo posea.
- De especial manera se recomienda a los directivos de Oscus Matriz, proveer a la sucursal de un dispositivo que genere energía, para seguir operando por lo menos 60' minutos después de un apagón.
- Se recomienda a los técnicos de Oscus Matriz, monitorear el uso que se les está dando a los computadores disponibles en la Sucursal Latacunga.
- Se recomienda reemplazar los equipos en los departamentos de secretaría y gerencia, en especial el terminal de secretaría puesto que ante la carga de trabajo que se debe ejecutar en este departamento se hace evidente la necesidad de reemplazar el computador por uno de mayor capacidad.

- Es recomendable realizar Auditoría Informática interna o externa, de forma periódica con el objetivo de prevenir desafortunados incidentes dentro de la sucursal.

ANEXOS

ANEXO No 4

Entrevista realizada al gerente de la sucursal Latacunga, fotografías de las entrevistas



UNIVERSIDAD TÉCNICA DE COTOPAXI
COOPERATIVA DE AHORRO Y CRÉDITO OSCUS Ltda. SUCURSAL
LATACUNGA

ENTREVISTA AL Sr. Ing. Marco Hidalgo Gerente de la sucursal Latacunga.

Objetivo de la encuesta: Obtener información general de la Sucursal Latacunga.

Responsable: Egda. Silvana Monge

Sr. Gerente le rogamos responda con la mayor sinceridad posible.

1.- La contratación del personal de Oscus se la hace en forma directa o a través de terciarizadoras?

3.- ¿En los contratos de trabajo se toma en cuenta vacaciones de los empleados?

4.- ¿En caso del personal femenino se respeta horas de maternidad y lactancia?

5.- ¿Se capacita al personal de Oscus a nivel informático?

6.- ¿Se ha realizado una evaluación de coherencia de cargos dentro de la sucursal?

Silvana Monge

Ing. Marco Hidalgo.

ANEXO No 6

Entrevista realizada al Ing. Carlos Santamaría, jefe del área informática, fotografías de las entrevistas.



UNIVERSIDAD TÉCNICA DE COTOPAXI
COOPERATIVA DE AHORRO Y CRÉDITO OSCUS Ltda. SUCURSAL
LATACUNGA

ENTREVISTA AL ING. CARLOS SANTAMARÍA JEFE DEL AREA DE SISTEMAS INFORMATICOS EN LA MATRIZ DE OSCUS.

Objetivo de la entrevista: Evaluar el desarrollo y prueba de los sistemas utilizados en OSCUS Sucursal Latacunga.

Responsable: Egda. Silvana Monge

Sr. Jefe del Área de Sistemas Informáticos le rogamos responda con la mayor sinceridad posible.

- 1.- ¿Quiénes intervienen al diseñar un sistema?
- 2.- ¿Los analistas son también programadores, en que porcentaje?
- 3.- ¿Qué lenguaje o lenguajes conocen los analistas?
- 4.- ¿Cuántos analistas hay y que experiencia tienen?
- 5.- ¿Qué lenguajes conocen los programadores?
- 6.- ¿Cómo se controla el trabajo de los analistas y programadores?
- 7.- ¿Se prueba la corrida de sistemas adquiridos y desarrollados?

ANEXO No 14

ENCUESTAS A LOS USUARIOS DEL SISTEMA

1.- ¿El sistema que está implementado en su institución cubre sus necesidades en forma?:

Deficiente () Regular () Aceptable ()

2.- Existen caídas del sistema:

Ocasionalmente () Siempre () Rara vez () Nunca ()

3.- ¿La seguridad establecida en el sistema es?

Deficiente () Regular () Aceptable () Excelente ()

4.- ¿La capacitación o asesoría informática brindada en su institución la considera?

Deficiente () Aceptable () Satisfactorio ()
Excelente ()

5.- Considera que la red implementada en su institución funciona:

Deficiente () Regular () Aceptable () Excelente ()

6.- El Hardware y Software que utiliza lo considera:

Deficiente () Regular () Aceptable () Excelente ()

7.- ¿El mantenimiento que le prestan a su equipo lo considera?

Deficiente () Regular () Aceptable () Excelente ()

8.- ¿Para mejorar el sistema informático qué le sugiere a la institución?

Que el sistema sea más rápido ()

Que se incrementen las medidas de seguridad ()

ENCUESTAS A LOS SOCIOS DE OSCUS

1.- ¿El sistema que se usa en su Cooperativa lo considera?:

Deficiente () Regular () Aceptable () Excelente ()

2.- ¿Qué piensa sobre la atención que brindan los empleados de Oscus a sus socios?

Deficiente () Regular () Aceptable () Excelente ()

3.- La forma en que desempeñan sus labores los empleados de Oscus la considera:

Deficiente () Regular () Aceptable () Excelente ()

4.- ¿La atención a sus demandas de información como saldos, estados de cuenta, etc. la considera:

A tiempo () Retrasada () Muy retrasada () No la recibe ()

NOTA: Para el desarrollo del presente trabajo investigativo se aplicaron algunos formularios, con el objetivo de obtener datos, los cuales están contenidos en un CD de datos anexo al empastado de tesis, también en éste se presentan algunos resultados del cumplimiento de las actividades de auditoria.

GLOSARIO

A:

AICPA (American Institute of Certified Public Accountants). - Instituto Americano de Certificación de Contadores Públicos.

Alcance de la auditoría.- Concretar la naturaleza y extensión del trabajo realizado:

Anchos de Banda.- En comunicaciones analógicas, la diferencia entre la frecuencia más alta y la más baja en un intervalo determinado.

Amenazas.- Normalmente, los conceptos amenaza y riesgo se presentan como conceptos sinónimos.

Aplicación.- Actividad específica que hace uso de un computador.

Arranque (bootstrap).- El proceso que usa el computador, al ser energizado para cargar el sistema operacional.

Auditor informático Es el responsable para establecer los objetivos de control que reduzcan o eliminen la exposición al riesgo de control interno.

B:

Back-Up.- Respaldo de la información.

Batch.- Proceso informático que se ejecuta fuera del acto de la recepción de datos.

Base de datos.- Conjunto de datos que afectan a una serie de aplicaciones o programas, que se construye para facilitar la actualización de datos.

Bicho (bug).- Un problema que aparece bien sea en el hardware o en el software del computador.

C:

Check list.- Cuestionario que se utiliza como metodología para realizar auditorías informáticas y otro tipo de pruebas.

Cinta magnética.- Medio de almacenamiento magnético.

Clave.- Campo identificador de un registro que se utiliza para localizar o clasificar información.

Cocomo.- por su nombre en Ingles (Constructive, Cost, Model) modelo constructivo de costos

Codificación.- Técnica para resguardar los datos de acceso no autorizados. Se utiliza un software o un dispositivo especial.

Código fuente.- Instrucciones escritas en un lenguaje con nivel de fuente

CONSEP.- consejo nacional de sustancias estupefacientes y psicotrópicas

Contraseña (Password).- Grupo de caracteres que se introduce en un sistema mecanizado por un usuario de terminal para que se le permita acceder a un programa

Control de validación.- Una técnica de control utilizada para detectar datos de entrada inexactos, incompletos o sin sentido.

Cracker: Realmente es a esta clase de personaje al que nos estamos refiriendo cuando hablamos de pirata informático.

D:

Datos de prueba.- Datos que se preparan exclusivamente para probar la exactitud de los programas y la lógica de los sistemas.

Default.- Cuando una cosa es hecha por defecto.

Diskette.- Un disco plástico móvil y flexible. Se lo utiliza, con frecuencia, como dispositivo de almacenamiento secundario en los microcomputadores.

E:

Eficacia.- La productividad y el servicio se cumplen en la cantidad y calidad esperada y sea útil.

Eficiencia.- Cuando una actividad maximiza el resultado de un insumo o lo minimiza.

Ejecutar.- Llevar a cabo una operación o un programa.

Entrada.- La información que entra al sistema de procesamiento de datos. **Equipos**

H:

Hacker.- Pirata informático.

Hardware.- Las partes físicas de un sistema de procesamiento de datos. Esto puede incluir un TRC, los manejadores de disco y la impresora, entre otros.

I:

Identificador del usuario (User ID).- Código de identificación asignado a un individuo o grupo de individuos.

Informática.- Es la ciencia del tratamiento racional de la información por medio de máquinas automáticas.

L:

Lenguaje/código fuente.- Lenguaje en el cual son escritos los programas de computador.

M:

Memoria.- La parte del computador que se usa para almacenar instrucciones (programas y datos).

Modem.- "Modulador/Demodulador" dispositivo que transforma las pulsaciones eléctricas del computador.

N:

No-Brake (UPS).- Equipo de suministro de energía que controla un banco de baterías y una planta de energía, en el momento de una suspensión de energía eléctrica, el sistema No-Brake o UPS.

Netbios.- Sistema de entrada y salida en la red usado por las aplicaciones API en una IBM, al requerir servicios de los procesos de la red. Estos servicios pueden incluir establecimiento de sesión y terminación; traslado de la información.

P:

PAD.- Procesamiento Automático de Datos o Area de Procesamiento de Datos.

Periférico.- Máquina o aparato auxiliar que esta bajo el control de la unidad central de proceso (por ejemplo, una impresora).

Procesos.- Son las etapas a pasos ordenados que conforman un ciclo transaccional o ciclo de actividad.

Programa.- Un conjunto de instrucciones y rutas de máquina para manejar una tarea de procesamiento de datos.

Protocolo.- Conjunto de normas y convenciones para enviar información a través de una red. Estas normas rigen el contenido, el formato, la temporización, la secuencia y el control de errores de los mensajes intercambiados entre los dispositivos de la red.

Protocolo de resolución de direcciones (ARP).- En TCP/IP, protocolo que utiliza tráfico de difusión en la red local para convertir una dirección IP asignada de forma lógica en su dirección física de nivel de control de acceso al medio o de hardware.

Protocolo de transferencia de archivos (FTP).- Miembro del conjunto de protocolos TCP/IP que se utiliza para copiar archivos entre dos equipos en Internet. Ambos equipos deben admitir sus funciones FTP correspondientes: uno debe ser un cliente FTP y el otro un servidor FTP.

Protocolo de transferencia de hipertexto (HTTP).- Protocolo utilizado para transferir información en el World Wide Web. Una dirección HTTP (un tipo de Localizador de recursos universal o dirección URL) tiene el siguiente formato:
<http://www.microsoft.com>.

Protocolo HTTPS.- Versión mejorada del http.

Protocolo de mensajes de control de Internet (ICMP).- Protocolo de mantenimiento del conjunto de protocolos TCP/IP que informa acerca de errores y ofrece una capacidad de conexión simple. La herramienta Ping utiliza ICMP para solucionar problemas de TCP/IP.

Protocolo de mensajes de control de Internet (ICMP).- La herramienta Ping utiliza ICMP para solucionar problemas de TCP/IP.

Protocolo IMAP.- IMAP (Internet Mail Access Protocol) permite a los usuarios acceder a sus e-mails directamente en el servidor

Protocolo de Internet (IP).- Protocolo de enrutamiento del conjunto de protocolos TCP/IP responsable de la asignación de direcciones IP, el enrutamiento y la fragmentación y ensamblaje de paquetes IP.

Protocolo NBS.- Bufete nacional de normas, conocido ahora como NIST.

Protocolo POP3.- El POP3 (Post Office Protocol versión 3) es un protocolo utilizado por los programas de correo electrónico para leer y almacenar localmente los mensajes desde el servidor.

Protocolo simple de transferencia de correo (SMTP).- Miembro del conjunto de protocolos TCP/IP que controla el intercambio de correo electrónico entre agentes de transferencia de mensajes.

Protocolo simple de administración de redes (SNMP).- Protocolo de red utilizado para administrar las redes TCP/IP. En Windows, el servicio SNMP se utiliza para proporcionar información de estado acerca de un host de una red TCP/IP.

Protocolo SSH.- SSH es un protocolo que permite establecer conexiones seguras, básicamente facilita un terminal para ejecutar comandos en forma remota a un servidor. A diferencia de telnet, SSH facilita un canal de datos encriptado.

Protocolo de control de vínculo (TCP).- Protocolo de control PPP que negocia parámetros de vínculo y PPP para configurar dinámicamente el nivel de vínculo de datos de una conexión PPP.

Protocolo de control de transporte/Protocolo de Internet (TCP/IP).- Conjunto de protocolos de red muy utilizados en Internet que permiten la comunicación entre redes interconectadas formadas por equipos con distintas arquitecturas de hardware y sistemas operativos. TCP/IP incluye estándares para la comunicación entre equipos y convenciones para conectar redes y enrutar las transmisiones.

Protocolo TELNET.- Telnet puede ser utilizado para conectarse a un equipo remoto , un dispositivo de red o una red TCP/IP privada.

R:

Recursos.- Son los elementos humanos o materiales involucrados en la realización de los ciclos transaccionales o de actividad. **Red.-** Grupo de computadores o terminales interconectados por medio de una instalación de transmisión.

Respaldo (back-up).- Es una reserva compatible, en forma de acceso de hardware, programas o copias de archivos, para utilizar en el caso de averías o caídas.

Riesgo.- Es la consecuencia directa de la materialización de una amenaza.

ROM (Read Only Memory).- Memoria de contenido fijo y, por tanto inalterable, que contiene las instrucciones fundamentales para hacer funcionar la máquina. Forma parte del sistema operativo.

S:

Sistema.- Es un trabajo del hombre que consiste de una colección de software y documentos que se relacionan a éste.

Sistemas operativos.- Engloba los Subsistemas de Teleproceso, Entrada/Salida, etc.

Software (SW).- Conjunto de programas que instruyen al computador para el acceso, procesamiento y almacenamiento de datos.

T:

Terminal.- Un dispositivo de entrada/salida tal como un TRC, un teletipo o una impresora.

U:

Usuario.- Persona o departamento que utiliza el sistema automatizado para procesar datos y producir información.

V:

Validación.- Verificación programada de datos o resultados, para asegurarse que cumplen unas normas predeterminadas.

Verificación.- Proceso de comprobar la exactitud de los datos que se han tecleado, con base en los que teclee otro operador, en un sistema que esté diseñado para indicar las diferencias que existan entre las dos operaciones del teclado.

Virus informáticos Es un medio que sirve para destruir, alterar, inutilizar o para dañar de cualquier modo los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

BIBLIOGRAFIA

BASICA

A:

ANDRADE, Santamaría Jorge, (2.004) Guía para el diseño del trabajo de grado,

B:

BAUDES, Gabriel, pagina de Internet.

BOCH GARCÍA, Carlos. *La Tesis Profesional*, editorial Pormaca, México 2002

C:

CASTRO, Julián, (2003) Manual de Auditoría Informática

CATACORA, Carpio Fernando,(1.998) Manual de Auditoría Informática

Contraloría General del Estado, Normas para Control Interno en el Área de Procesamiento de Datos, Boletín Jurídico No 6.

D:

Diccionario de informática, editorial Grafillés, impreso en Madrid España, edición 2001

G:

GARY G., Bitter. *Informática y Computación*, ediciones Alfa Nauta, impreso en España, Programa educativo temático, edición 2000

GUTIÉRREZ SAENZ, Raúl y SANCHEZ GONZÁLES José. *Metodología del trabajo intelectual*, editorial Esfinge, México 1990.

H:

HOLGRUN, Hayashi, Elementos de muestreo y correlación, Textos universitarios, Mexico, 1974

HOPKINS, Kenneth D. Estadística Básica para las Ciencias Sociales y del Comportamiento. editorial Limusa , ttercera edición, Mexico 1.998

L:

LINNINGER A., Charles y WARWICK P. Donald, la encuesta por muestreo, teoría y práctica, Compañía Editorial Continental, México, 1978

CITADA

M:

MAZZAL Miguel, (2001) El mundo de la Auditoria Informática.

MENDENHALL, William y REINMUNTH, James, Estadística para administración economía, Wadswrtl, Massachussets, 1981.

MOLINARI Agustín, (1999) Auditoría Informática

P:

PORTER, Thomas Jr., Auditoría de Sistemas Electrónicos, ediciones Trilla segunda edición, Mexico 1998.

R:

RIOS, Villafuerte Wellington, Auditoria Informática Guía Para su Aplicación. Corporación Edi-Abaco CIA. LTDA. Quito Ecuador, 2000.

S:

SANCHEZ, Mario, Guía para la Auditoría de Sistemas de Procesamiento de Datos, ediciones Pelicano, primera edición, 2000

T:

THOMAS, H. Wonnacott, Introducción a la Estadística, editorial Limusa S.A. 1999.

INTERNET

W:

WATERHOUSE, Price, El Auditor y los Sistemas Automáticos de Procesamiento de Datos, ediciones Centauro, 1.997.

WWW.google.auditoria.informatica.com

Fuente:wwwgoogle/cooperativismo/fundamentosdelcooperativismo fecha: 22/01/2002

WWW.monografias.auditoria.informatica.com

WWW.Google.auditoria.informatica.com

www.monografias/auditoriainformatica/conceptos.com

www.monografias.com/auditoriainformatica/conceptodeauditoríadesistemasdeinformación

WWW.Yahoo.auditoria.informatica.com