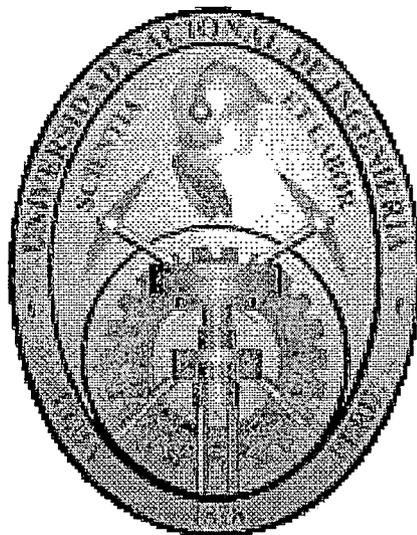


UNIVERSIDAD NACIONAL DE INGENIERIA
Facultad de Ingeniería Industrial y de Sistemas



**DESARROLLO DE LA AUDITORIA DE SISTEMAS EN LA GESTION
ADMINISTRATIVA Y ACADEMICA DE LA UNIVERSIDAD ANDINA
"NESTOR CACERES VELASQUEZ"**

TESIS PROFESIONAL

Para Optar el Título Profesional de :
INGENIERO DE SISTEMAS

JOSE ANTONIO ESPINAL TEVES

Digitalizado por:

**Consortio Digital del
Conocimiento MebLatam,
Hemisferio y Dalse**

LIMA – PERU
2001

DEDICATORIA:

Con Mucho cariño a mi Familia y a mis amigos.

AGRADECIMIENTO:

Jesucristo a ti las gracias por todo y a mis
queridos padres y hermanos .

INDICE

	Pág.
CAPITULO I	
INTRODUCCIÓN	1
1.1 Tematización	1
1.2 Problema	2
1.2.1 Planteamiento del Problema	2
1.2.2 Importancia	3
1.2.3 Objetivos	4
1.2.3.1 Objetivo General	4
1.2.3.2 Objetivo Específico	4
1.2.4 Metodología de la Investigación	5
1.2.4.1 Tipo de Investigación	5
1.2.4.2 Area de Investigación	5
1.2.4.3 Ubicación del Estudio	6
 CAPITULO II	
MARCO TEORICO	7
2.1 Antecedentes	7
2.1.1 Marco Legal	8
2.2 Hipótesis	9
2.2.1 Hipótesis General	9
2.2.2 Hipótesis Específicas	9
2.3 Auditoría de Sistemas	10
2.3.1 Definición	10
2.3.2 Objetivos	11
2.3.3 Perfil del Auditor	15
2.3.4 Actividades Principales	16
2.4 Metodología para el desarrollo de la Auditoría de Sistemas	
Orientada al Análisis de Riesgos	19
2.4.1 Riesgo en la continuidad del proceso	22

2.4.2	Riesgo en la eficacia del servicio	22
2.4.3	Riesgo en la eficiencia del servicio	23
2.4.4	Riesgos económicos directos	23
2.4.5	Riesgos de la seguridad lógica	23
2.4.6	Riesgos de la seguridad física	24
2.5	Etapas para el desarrollo de la Auditoría de Sistemas	24
2.5.1	Etapas 1: Cuestionarios	25
2.5.2	Etapas 2: Identificar los riesgos	25
2.5.3	Etapas 3: Calcular el impacto	25
2.5.4	Etapas 4: Creación de los informes	25
2.5.5	Plan de Contingencia	25
2.5.5.1	Descripción del Plan de Contingencias	25
2.6	Aplicación de Técnicas y Herramientas de Auditoría	27
2.6.1	Aplicación de técnicas	27
2.6.1.1	Pruebas de Controles	27
2.6.1.2	Pruebas Sustantivas	28
2.6.1.3	Prueba de Integridad de Datos	30
2.6.1.4	Auditabilidad de Sistemas	31
2.6.2	Aplicación de Herramientas	33
2.6.2.1	Prueba Unitaria	33
2.6.2.2	Prueba de Integración	34
2.6.2.3	Pruebas de Verificación	34
2.6.2.4	Prueba de carga máxima	43
2.6.2.5	Prueba de almacenamiento	43
2.6.2.6	Prueba de tiempo de ejecución	43
2.6.2.7	Pruebas de Seguridad	43
2.6.2.8	Pruebas de Resistencia	44
2.6.2.9	Pruebas de Recuperación	44
2.6.2.10	Pruebas de Procedimientos	44
2.6.2.11	Pruebas de Factores Humanos	44
2.6.3	Técnicas de Auditoría de Sistemas en Funcionamiento	44
2.6.3.1	Técnicas Administrativas	45

2.6.3.2	Técnicas para probar controles de sistemas en funcionamiento	48
2.6.3.3	Técnicas para seleccionar y monitorear transacciones	53
2.6.3.4	Técnicas para el examen de archivos	57
2.6.3.5	Técnicas para examinar programas aplicativos	59
2.7	Elaboración del Informe Final	64
2.7.1	Estructura del Informe Final de Auditoría	65
2.7.1.1	Introducción del Informe Final	66
2.7.1.2	Conclusiones	68
2.7.1.3	Observaciones	69
2.7.1.4	Recomendaciones	71
2.7.1.5	Firma del Informe	73
2.7.1.6	Anexos	73

CAPITULO III

APLICACIÓN DE LA METODOLOGÍA DE ANALISIS DE RIESGOS

3.1	ETAPA 1: Diseño de Cuestionarios	74
3.1.1	Encuesta a Usuarios	74
3.1.2	Entrevista al Centro de Computo	79
3.1.3	Control de Operación	84
3.1.4	Controles de Salida	90
3.1.5	Orden en el Centro de Computo	91
3.1.6	Evaluación de la configuración en el Centro de Computo	92
3.1.7	Seguridad Lógica, Física y Confidencial	94
3.1.7.1	Seguridad Física	94
3.1.7.2	Seguridad en la utilización del equipo	104
3.1.7.3	Seguridad al restaurar el equipo	106
3.1.7.4	Procedimientos de respaldo en el caso de desastre	107
3.1.8	Formularios para el seguimiento y control de la Auditoría de Sistemas	109

DESCRIPTORES TEMATICOS

- AUDITORIA DE SISTEMAS
- UNIVERSIDAD ANDINA NESTOR CACERES VELASQUEZ
- METODOLOGIA
- TECNICAS DE AUDITORIA DE SISTEMAS EN FUNCIONAMIENTO
- NORMAS DE CONTROL
- ETAPAS DE LA AUDITORIA
- EVALUACION DE RIESGOS
- CREACION DE INFORMES

Sumario

La aplicación de la Auditoría de Sistemas en la Universidad Andina “Nestor Cáceres Velasquez” , el mismo que permitirá ser una herramienta de seguridad y control de los Organos de Auditoría Interna de las Organizaciones que tienen como función principal el Control Interno, bajo la dirección de la Contraloría General de la República El presente informe presenta en su primera parte la metodología para el desarrollo de la Auditoría de Sistemas y en la Segunda Parte, la puesta en marcha de la aplicación de la metodología de la Auditoría de Sistemas que permitirá verificar que el Area de Sistemas se haya realizado con economía, eficacia y transparencia sobre la correcta utilización de los recursos informáticos buscando además los niveles de calidad de seguridad y control de la información logrando así cumplir con los objetivos de la Institución

José Antonio Espinal Teves

CAPITULO I

INTRODUCCION

1.1 Tematización.

La auditoría de Sistemas 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.

La auditoría de Sistemas deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoría de Sistemas informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).

1.2 Problema

1.2.1 Planteamiento del Problema

La Universidad Andina Nestor Cáceres Velasquez es una Universidad Privada que se encuentra enclavada en el Altiplano a 3200 mt. sobre el nivel del mar, es una zona cosmopolita y comercial siendo esta la única Universidad en Juliaca - Puno, desde que fue fundada en el año 1983 es una Universidad que imparte conocimientos a gran parte de los estudiantes altiplánicos, además cabe resaltar que las Universidad nace del esfuerzo conjunto del pueblo y las municipalidad de Juliaca en la gestión del Alcalde Luis Cáceres Velasquez y que posteriormente las gestiones fueron descuidando la administración de esta Universidad por la corrupción e ineficacia en los cargos, y como consecuencia ahora se encuentra pasando por un régimen de reestructuración administrativo y académico. Es aquí donde este trabajo pretende servir como herramienta para los órganos de control interno de la Universidad Andina.

Problemática de la Entidad

- Describir las causas que dificultan y retrasan el logro de los objetivos propuestos en los planes y programas de la Entidad, determinando las áreas críticas de la Entidad.
- El Organismo de Auditoría Interna analizará cada área crítica señalará la acción de control programada.

Problemática del Organismo de Auditoría Interna

- Señalar los principales problemas que afronta el OAI para el normal desarrollo de sus actividades.
- Indicar los requerimientos de capacitación.

1.2.2 Importancia

El presente informe presenta un desarrollo de la aplicación de la Auditoría de Sistemas en la Gestión Académica y Administrativa de la Universidad Privada Nestor Cáceres Velásquez de Juliaca - Puno, el mismo que permitirá ser una herramienta de seguridad y control de los Organismos de Auditoría Interna de la Organización que tienen como función principal el control de la UANCV, bajo la dirección del Rectorado y en especial a la Inspectoría General de la UANCV.

1.2.3 Objetivos

1.2.3.1 Objetivo General

Evaluar, verificar y comprobar el uso adecuado de los recursos informáticos de la entidad bajo los principios de economía, eficacia, eficiencia y transparencia la misma que se encuentre enmarcado en el cumplimiento de los objetivos y metas trazadas en los planes de la Institución.

1.2.3.2 Objetivos Específicos

Teniendo entre sus objetivos específicos los siguientes:

- Implementar el proceso que cumpla las políticas, normas y procedimientos institucionales y legales.
- Adecuar el procedimiento para la selección, uso y resguardo de los activos físicos y lógicos.
- Consistenciar los sistemas y de las aplicaciones desarrolladas.
- Asegurar una adecuada y eficaz operación de los sistemas y de las aplicaciones desarrolladas
- Detectar deficiencias en busca de las mejoras en los recursos informáticos que se utilizan en la organización, incluyendo los servicios prestados por terceros y que permitan con el informe final, efectuar acciones preventivas y correctivas para eliminar las fallas y carencias que se detecten.
- Salvaguardar físicamente los equipos de Hardware.
- Verificar y evaluar.

- Proteger los activos de la Organización.

1.2.4 Metodología de la Investigación

Es el conjunto de actividades que se realizan para obtener nuevos conocimientos, a partir de los provisoriamente establecidos y sistematizados anteriormente.

1.2.4.1 Tipo de Investigación

- APLICATIVO

1.2.4.2 Area de Investigación

- **Administrativa**
 - Vice- Rectorado Administrativo
 - Bienestar Universitario
 - Asistencia Social, Salud y Servicios
 - Contabilidad
 - Tesorería
 - Abastecimiento y Patrimonio
 - Personal
 - Remuneraciones
 - Control de Personal

- **Académico**
 - Vice- Rectorado Académico
 - Oficina de Servicios Académicos
 - Oficina Permanente de Admisión
 - Oficina de Investigación
 - Centro preuniversitario
 - Oficina de Extensión Universitaria y Proyección Social.

1.2.4.3 Ubicación del Estudio

- **Localización**
 - UNIVERSIDAD ANDINA “NESTOR CÁCERES
VELASQUEZ”
 - DEPARTAMENTO DE PUNO
 - PROVINCIA DE SAN ROMAN
 - DISTRITO DE JULIACA

CAPITULO II

MARCO TEORICO

2.1 Antecedentes

La Universidad Andina Nestor Cáceres Velasquez, surgió gracias al trabajo esforzado de un grupo de Autoridades de la Provincia de San Román y gracias a la juventud estudiosa preocupada por superarse conforme a la ciencia y la tecnología.

Logro su Ley de Creación N° 23733 promulgado el 28 de diciembre de 1983 y su Ley complementaria N° 24661. El 10 de julio de 1992 por Resolución N° 1287-92-ANR de la Asamblea Nacional de Rectores se le otorgó autorización de funcionamiento definitivo, disponiendo la constitución de sus órganos de Gobierno logrando así su incorporación definitiva al sistema de Universidad Peruana.

2.1.1 Marco Legal

La Universidad Andina Nestor Cáceres Velasquez se rige por el Sistema Nacional de Control regulado por el D.L. 26162, teniendo como organismo la Asamblea Nacional de Rectores, el cual autorizó su funcionamiento como una empresa privada de servicios educativos; así como la Contraloría General de la República que realizó la Auditoría Gubernamental para verificar que la gestión Universitaria se haya realizado con economía, eficiencia, eficacia y transparencia de conformidad con las disposiciones legales aplicables. Las Normas contribuyen a que las auditorías sean evaluaciones imparciales, objetivas y confiables, con base en las:

- a. Normas Generales del Perú (Anexo N° 05)
- b. Normas y Disposiciones de la Contraloría General de la República. (Anexo N°06)
- c. Normas del Instituto Nacional de Defensa de la Competencia y Protección de la Propiedad Intelectual INDECOPI (Anexo N°07)
- d. Normas del Instituto Nacional de Estadística e Informática INEI (Anexo N°08)
- e. Normas de Auditoría Generalmente Aceptada (NAGA)
- f. Normas Internacionales de Auditoría (NIA)
- g. Normas de la Organización Internacional de Instituciones Supremas de Auditoría (INTO SAI)

La Contraloría General de la República del Perú ha establecido:

- Normas de Auditoría Gubernamental (NAGU), adaptándola en lo aplicable a la ley del Sistema de Control. Las NAGU, son de cumplimiento obligatorio y aplicación indispensable para los auditores de la Contraloría General de la

República, de los órganos de Auditoría Interna y de las sociedades de Auditoría cuando sean decisiones para efectuar Auditorías Gubernamentales.

- Igualmente los profesionales y/o especialistas estarán obligados bajo responsabilidad a sujetar su accionar a las NAGU en lo que resulte aplicable.

2.2 Hipótesis

2.2.1 Hipótesis General

La Auditoría de Sistemas en la Universidad Andina Nestor Cáceres Velásquez (UANCV) optimiza beneficios, detecta anomalías y sugiere medidas correctivas proponiendo un modelo estándar de premisas para describir situaciones de riesgo.

2.2.2 Hipótesis Específicas

- La Auditoría de Sistemas verifica si hay una política de control.
- La Auditoría de Sistemas verifica si la planificación del Centro de Cómputo tiene coherencia con el plan estratégico de la UANCV.
- La Auditoría de Sistemas verifica la existencia del desarrollo de sistemas.
- La Auditoría de Sistemas verifica si se cumple con las normas de control y soporte de los recursos de información.
- La Auditoría de Sistemas verifica responsabilidades sobre el acceso seguridad, mantenimiento y control de hardware.
- La Auditoría de Sistemas verifica que el software existente cuente con procedimientos de acceso, seguridad, mantenimiento y control.

- La Auditoría de Sistemas verifica si la organización funciona adecuadamente.
- La Auditoría de Sistemas verifica si los recursos humanos son suficientes.
- La Auditoría de Sistemas verifica la existencia de estándares y documentación.
- La Auditoría de Sistemas verifica los planes del sistema.
- La Auditoría de Sistemas verifica la demanda insatisfecha del sistema de computación y de información de las áreas.
- La Auditoría de Sistemas verifica la atención a los usuarios por parte del centro de cómputo.
- La Auditoría de Sistemas verifica los contratos de licencia de Uso de Software.
- La Auditoría de Sistemas verifica la adquisición correcta del Hardware.
- Simplifica procesos redundantes.
- Advierte de peligros por falta de seguridad.

2.3 Auditoría de Sistemas

2.3.1 Definición

La auditoría de sistemas es una rama de la Auditoría de Gestión u Operativa a la Entidad y se ocupa de la verificación, revisión y evaluación de los controles de los recursos informáticos tanto de sistemas, equipos de computo, procedimientos y funcionamiento del Area de Sistemas y de la Organización que permita la seguridad y confiabilidad que se le puede atribuir a la información que se procesa y produce en los

diferentes sistemas de la Organización, así como de su utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

Verifica la existencia y aplicación de todas las normas y procedimientos establecidos, así como minimiza las posibles causas de riesgos tanto en las instalaciones, equipos, sistemas y datos que se manipulan en la Organización.

También, es el examen que se realiza en los ambientes que cuentan con equipos de procesamiento electrónico de datos y que, por las características de este ambiente se deben adecuar los procedimientos, las técnicas y las herramientas de auditoría a los cambios sustanciales que presenta dicho ambiente.

2.3.2 Objetivos

Evaluar, verificar y comprobar el uso adecuado de los recursos informativos de la entidad bajo los principios de economía, eficacia, eficiencia y transparencia la misma que se encuentre enmarcado en el cumplimiento de los objetivos y metas trazadas en los planes de la Institución.

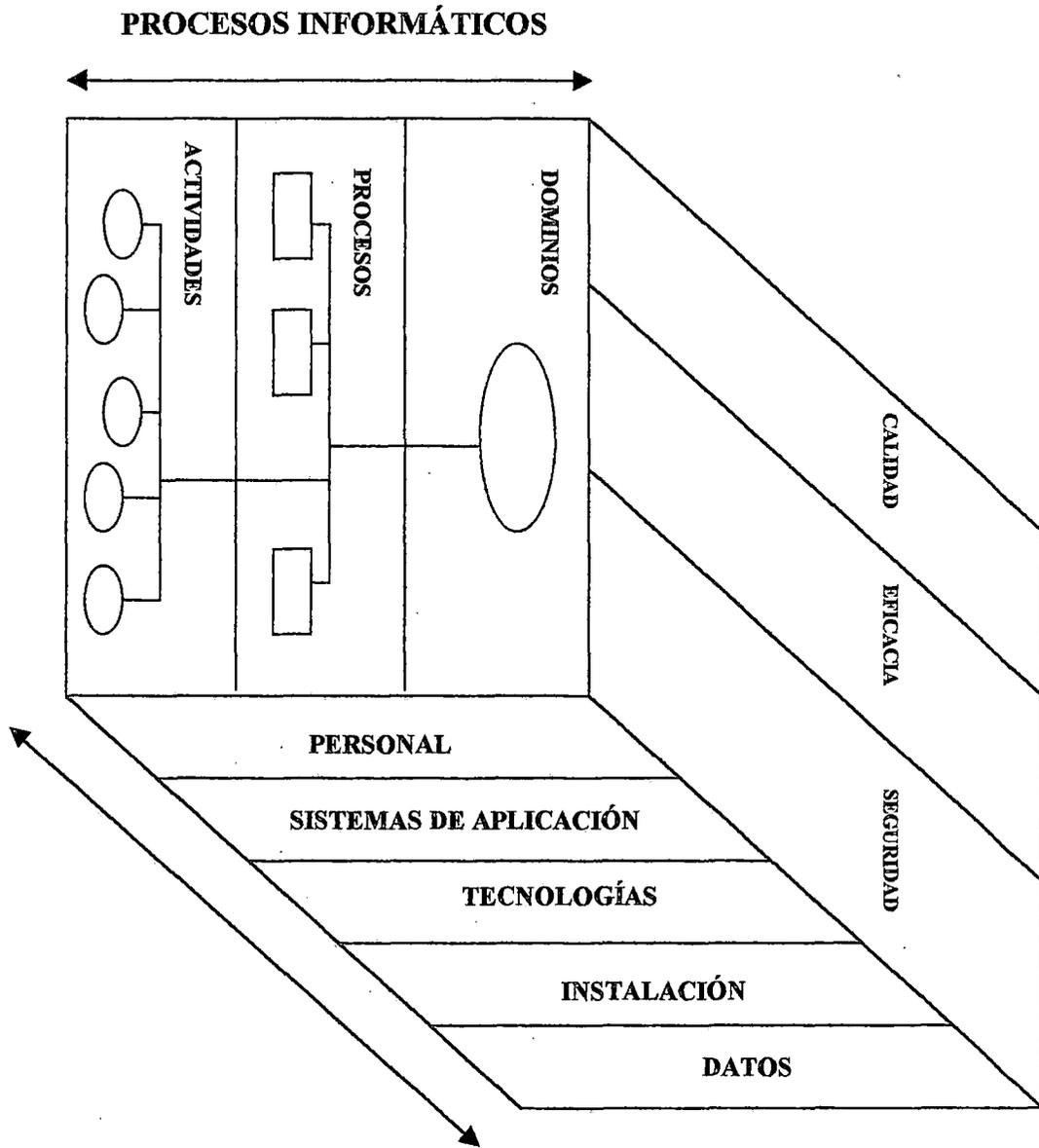
Teniendo entre sus objetivos específicos los siguientes:

- Que la implementación del proceso cumpla las políticas, normas y procedimientos institucionales y legales.
- Que exista un adecuado procedimiento para la selección, uso y resguardo de los activos físicos y lógicos.

- Que se controle la consistencia y confiabilidad de los sistemas y de las aplicaciones desarrolladas.
- Que se asegure una adecuada y eficaz operación de los sistemas y de las aplicaciones de información de la entidad.
- Promover hacia el mejoramiento de los sistemas de control y calidad de la información generada por los recursos informáticos.
- Realizar evaluaciones de los sistemas informáticos y emitir informes al respecto.
- Proponer nuevas normas o modificar las existentes para la evaluación de los recursos informáticos.
- Proteger los activos de la Organización.
- Salvaguarda física.
- Verificación y evaluación.

Para el cumplimiento de los objetivos, el auditor de sistemas aplicara un conjunto de técnicas y herramientas, dependiendo del ambiente donde se desenvuelva que le permita detectar deficiencias en busca de mejoras en los recursos informáticos que se utilizan en la Organización, incluyendo los servicios prestados por terceros y que permitan con el informe final, efectuar acciones preventivas y correctivas para eliminar las fallas y carencias que se detecten.

CUBO DE AUDITORÍA



MARCO REFERENCIAL DE OBJETIVOS DE CONTROL PARA LA TECNOLOGIA DE LA INFORMACION



2.3.3 Perfil del Auditor

a. Conocimiento del Negocio

- Experiencia en la Industria
- Conocimiento de la Empresa
- Dominio de los objetivos generales y sectoriales
- Identificación de la áreas críticas.

b. Conocimiento de Auditoría

- Control Interno
- Métodos Estadísticos
- Enfoque de Auditoría Global
- Auditoría asistida por computadora
- Técnicas de Auditoría.

c. Conocimiento de Procesamiento de datos

- Equipos (Hardware)
- Programas de base (Software)
- Programas de Aplicación.
- Organización de Procesamiento de datos
- Producción de procesamiento de datos
- Seguridad de datos.

d. Capacidad de Comunicación

- Interpersonal (oral y escrito) con los gerentes subordinados, personal de PED y los usuarios.
- Capacidad para escuchar y comprender la posición de los auditados.

e. Capacidad Gerencial

- Liderazgo
- Madurez
- Sentido del Negocio.

f. Experiencia en Auditoría

- Obtención de Recursos
- Uso de Expertos
- Planeamiento y Desarrollo de programas y planes.
- Capacidad de negociación y venta de propuestas.
- Control de calidad de la tarea de auditoría.
- Elaboración de informes especiales
- Capacidad para generar alternativas.

2.3.4 Actividades Principales

El auditor debe tener la habilidad para revisar y probar la integridad de los sistemas siendo sus actividades principales:

- a. Verificar los controles y procedimientos de autorización de la utilización y captura de los datos, su proceso y salidas de información, así como los programas que las generan. Es importante revisar los procedimientos para el mantenimiento de los programas y las modificaciones a los sistemas.
- b. Revisar las transacciones realizadas para asegurarse de que los archivos reflejan la situación actual.
- c. Revisar las transacciones y los archivos para detectar posibles desviaciones de las normas establecidas.
- d. Asegurarse de que las aplicaciones cumplan con los objetivos definidos en la plantación.
- e. Revisar todos los cambios hechos a los programas y sistemas para verificar la integridad de las aplicaciones.

Todos los programas o paquetes empleados en la auditoría deben permanecer bajo estricto control del departamento de auditoría, dentro de los papeles de trabajo. Por esto, toda la documentación, material de pruebas, listados fuente, programas fuente y objeto, además de los cambios que se les hagan, serán responsabilidad del auditor.

QUÉ PUEDEN / DEBEN HACER LOS AUDITORES	QUÉ NO DEBEN HACER LOS AUDITORES
Ser independientes y objetivos	Actuar en beneficio propio por encima del interés del cliente
Recomendar	Obligar, forzar, amenazar
Ser competentes en la materia seguridad)	Asumir encargos para los que no estén preparados
Basar sus informes en verificaciones y evidencias	Basarlos en suposiciones
Verificar que se evalúan periódicamente riesgos o bien evaluarlos	Revisar la seguridad "día a día" o administrarla (son funciones de otros)
Conocer perfiles de usuarios	Realizar gestión perfiles de usuarios
Conocer criterios y prácticas sobre contraseñas	Gestión/asignación contraseñas o conocerlas
Verificar que las aplicaciones se desarrollan y mantienen según normas y se incorporan controles	Realizar funciones de análisis o gestionar proyectos
Revisar codificación de programas (seguridad y calidad) y las pruebas realizadas, o bien probarlos	Codificar programas
Revisar la documentación (aplicaciones, programas)	Realizar la documentación.
Verificar que siguen los procedimientos	Escribir procedimientos
Responsabilizarse del contenido de sus informes	Aceptar presiones de sus jefes o clientes y que el informe no sea veraz
Evaluar riesgos e informes	Garantizar que no se puedan realizar/haber realizado delitos, fraudes o errores
Sustentar los informes con papeles de trabajo	Enzarsarse en discusiones de diferencias de opiniones
Estar al día en cuanto a avances, riesgos, metodologías	Auditar con técnicas, métodos o recomendaciones obsoletos.

También el Auditor podrá emplear como herramienta de trabajo la microcomputadora el mismo que constituye una herramienta que facilitara la realización de actividades de revisión como:

- a. Trasladar los datos del sistema a un ambiente de control del auditor
- b. Llevar a cabo la selección de datos
- c. Verificar la exactitud de los cálculos
- d. Muestreo estadístico
- e. Visualización de datos
- f. Ordenamiento de la información
- g. Producción de reportes e histogramas

2.4 Metodología para el desarrollo de la Auditoría de Sistemas Orientada al

Análisis del Riesgo

La metodología utilizada es la Evaluación de Riesgos (ROA Risk Oriented Approach) recomendada por ISACA (Information System, Audit and Control Association), Asociación Internacional de Auditores de Sistemas de Información. (ver Anexo N° 09)

Esta evaluación de Riesgos se desarrolla sobre determinadas áreas de aplicación y bajo técnicas de Checklist (Cuestionarios) adaptados a cada entorno específico; deberá tenerse en cuenta que determinados controles se repetirán en diversas áreas de

riesgo. Esto es debido a que dichos controles tienen incidencias independiente en cada una y, dado que se pretende poder analizar cada área independientemente, es necesaria dicha repetición. Asimismo los controles generales y algunos controles de características especiales, como pueden ser los de bases de datos, se aplicarán teniendo en cuenta las particularidades de cada entorno.

Esta metodología resulta más adecuada para la aplicación en esta organización antes que las metodologías: COSO, IFAC, IIA, ISACA, SAC, COBIT, por que estas otras son para corporaciones que cuentan con un alto nivel de sistemas automatizados, en el caso nuestro las necesidades son distintas y más elementales.

Están desarrolladas para la identificación de la falta de controles y el establecimiento de un plan de contramedidas en base a unos cuestionarios, se identifican vulnerabilidades y riesgos y se evalúa el impacto para mas tarde identificar las contramedidas y el coste.

PROS Y CONTRAS DE LAS METODOLOGIAS

CUANTITATIVAS Y CUALITATIVAS

	CUANTITATIVAS	CUALITATIVAS O SUBJETIVAS
<p>P</p> <p>R</p> <p>O</p> <p>S</p>	<ul style="list-style-type: none"> - Enfoca pensamientos mediante el uso de números. - Facilita la comparación de vulnerabilidades muy distintas. - Proporciona una cifra “justificante” para cada contramedida. 	<ul style="list-style-type: none"> - Enfoque lo amplio que se desee. - Plan de trabajo flexible y reactivo - Se concentra en la identificación de eventos. - Incluye factores intangibles
<p>C</p> <p>O</p> <p>N</p> <p>T</p> <p>R</p> <p>A</p> <p>S</p>	<ul style="list-style-type: none"> - Estimación de probabilidad depende de estadísticas fiables inexistentes. - Estimación de las pérdidas potenciales solo si son valores cuantificables. - Metodologías estándares - Dificiles de mantener o modificar - Dependencia de un profesional 	<ul style="list-style-type: none"> - Depende fuertemente de la habilidad y calidad del personal involucrado. - Pueden excluir riesgos significantes desconocidos. - Identificador de eventos reales mas claros al no tener que aplicarles probabilidades complejas de calcular. - Dependencia de un profesional.

- La tendencia de uso en la realidad, es la mezcla de ambas.

Tal y como hemos apuntado anteriormente, la autoguía está dividida en varias áreas de riesgo, concretamente siete, que son:

- 2.4.1 Riesgo en la continuidad del proceso.
- 2.4.2 Riesgo en la eficacia del servicio.
- 2.4.3 Riesgo en la eficiencia del servicio.
- 2.4.4 Riesgos económicos directos.
- 2.4.5 Riesgos de la seguridad lógica.
- 2.4.6 Riesgos de la seguridad física.

2.4.1 Riesgo en la continuidad del proceso

Son aquellos riesgos de situaciones que pudieran afectar a la realización del trabajo informático o incluso que pudieran llegar a paralizarlo, y, por ende, llegar a perjudicar gravemente a la empresa o incluso también a paralizarla. Se deberá hacer especial hincapié en el análisis estricto de estos riesgos puesto que, si bien otros podrían afectar relativamente a la empresa o bien causarle perjuicios de diverso tipo, éstos podrían ocasionar un verdadero desastre. No pretendemos ser alarmistas y, por supuesto, no todos los riesgos analizados llevan a paralizar la empresa, pero insistimos en tener muy en cuenta el análisis exhaustivo de estos riesgos.

2.4.2 Riesgos en la eficacia del servicio informático

Entenderemos como eficacia del servicio la realización de los trabajos encomendados. Así pues, los riesgos en la eficacia serán aquellos que alteren dicha

realización o que afecten a la exactitud de los resultados ofrecidos por el servicio informático.

2.4.3 Riesgo en la eficiencia del servicio informático

Entenderemos como eficiencia del servicio la mejor forma de realizar los procesos o trabajos, ya sea a nivel económico o técnico, pretendiendo con el análisis de estos riesgos mejorar la calidad de servicio. Hay que matizar en este aspecto que determinados controles podrían resultar una mejora considerable de la eficiencia del servicio pero igualmente podrían resultar económicamente poco rentables sobre todo los responsables de la empresa en cuya mano estará la decisión de aplicación de los mismos.

2.4.4 Riesgos económicos directos

En cuanto a estos riesgos se analizarán aquellas posibilidades de desembolsos directos inadecuados, gastos varios que no deberían producirse, e incluso aquellos gastos derivados de acciones ilegales con o sin consentimiento de la empresa que pudieran transgredir la normativa de la empresa o las leyes vigentes.

2.4.5 Riesgos de la seguridad lógica

Como riesgos en seguridad lógica entenderemos todos aquellos que posibiliten accesos no autorizados a la información mecanizada mediante técnicas informáticas o de otros tipos. Incluiremos igualmente aquellos inherentes a transmisiones pese a que

quizá en determinados ámbitos de aplicación podrían constituir un área independiente pero que se anexan con el fin de compactar el sistema de análisis.

2.4.6 Riesgos de la seguridad física

Los riesgos en cuanto a seguridad física comprenderán todos aquellos que actúen sobre el deterioro o apropiación de elementos de información de una forma meramente física.

Dadas estas áreas de riesgos, el usuario podrá valorar cada una independientemente según sus necesidades. Aún así, se consideran como más importantes, y casi podríamos asegurar que imprescindibles, las dos primeras:

- Riesgo en la continuidad del proceso
- Riesgo en la eficacia del servicio

Por lo que cualquier análisis debería ser comenzado con las mismas.

Todas estas áreas están incluidas en cada ámbito de aplicación de acuerdo con su especificidad según la división que dimos al principio de miniordenadores, redes locales y PCs.

2.5 Etapas para el desarrollo de la Auditoría de Sistemas

Están desarrolladas para la identificación de la falta de controles y el establecimiento de un plan de contramedidas. En base a unos cuestionarios, se

identifican vulnerabilidades y riesgos, y se evalúa el impacto para más tarde identificar las contramedidas y el coste. La siguiente etapa es la más importante, pues mediante un juego de simulación (que llamaremos ‘Que pasa si?...’) analizamos el efecto de las distintas contramedidas en la disminución de los riesgos analizados, eligiendo de esta manera un plan de contramedidas (plan de seguridad) que compondrá el informe final de la evaluación.

El esquema básico de una metodología de análisis de riesgos es, en esencia, el representado en:

- 2.5.1 Etapa 1: Cuestionarios.
- 2.5.2 Etapa 2: Identificar los riesgos.
- 2.5.3 Etapa 3: Calcular el impacto.
- 2.5.4 Etapa 4: Creación de los informes.
- 2.5.5 Plan de Contingencia.

2.5.5.1 Descripción del Plan de Contingencias

El auditor debe conocer perfectamente los conceptos de un plan de contingencias para poder auditarlo. El plan de contingencias y de recuperación de negocio es lo mismo, pero no así el plan de restauración interno. También se manejan a veces los conceptos de plan de contingencias informático y plan de contingencias corporativo, cuyos conceptos son sólo de alcance. El corporativo cubre no sólo la informática,

sino todos los departamentos de una entidad, y puede incluir también el informático como un departamento más. Frecuentemente, se realiza el informático.

El plan de contingencias es una estrategia planificada constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminada a conseguir una restauración progresiva y ágil de los servicios de negocio afectados por una paralización total o parcial de la capacidad operativa de la empresa. Esa estrategia, materializada en un manual, es el resultado de todo un proceso de análisis y definiciones que es lo que dá lugar a las metodologías.

Es muy importante tener en cuenta que el concepto a considerar es “la continuidad en el negocio”; es decir, estudiar “todo lo que puede paralizar la actividad y producir pérdidas”. Todo lo que no considere este criterio no será nunca un plan de contingencias. Veamos cuales son las fases de un plan:

- **Análisis y Diseño:** se estudia la problemática, las necesidades de recursos, las alternativas de respaldo, y se analiza el coste/beneficio de las mismas. Esta es la fase más importante, pudiendo llegarse al final de la misma incluso a la conclusión: de que no es viable o es muy costoso su seguimiento.
- **Desarrollo del Plan:** esta fase y la siguiente son similares en todas las metodologías. En ella se desarrolla la estrategia seleccionada, implantándose hasta el final todas las acciones previstas. Se definen las distintas

organizaciones de emergencia y se desarrollan los procedimientos de actuación generando, así, la documentación del plan. Es en esta fase cuando se analiza la vuelta a la normalidad, dado que pasar de la situación normal a la alternativa debe concluirse con la reconstrucción de la situación inicial antes de la contingencia, y esto es lo que no todas las metodologías incluyen.

2.6 Aplicación de Técnicas y Herramientas de Auditoría

El auditor de sistemas deberá tener conocimiento del mayor número de metodologías, técnicas y herramientas que le permitan realizar una labor adecuada de control, por lo que deberá reunir las herramientas necesarias que le permitan auditar las diferentes etapas de verificación y evaluación de la vida útil del sistema y de los recursos informáticos así como para la evaluación del área de sistemas, por lo que, en esta metodología se divide en:

2.6.1 Aplicación de técnicas.

2.6.2 Aplicación de Herramientas.

2.6.1. Aplicación de Técnicas:

2.6.1.1 Pruebas de Controles

Una vez identificada todos los controles existentes, el auditor debe identificar los controles importantes los mismos que pueden estar o no en los cuestionarios y controles incluidos en el programa de trabajo.

Para controles manuales, el auditor deberá identificar un documento fuente que pueda ser examinado y que contendrá dicha evidencia.

El auditor deberá considerar la aplicación de muestreos estadísticos cuando este diseñando las pruebas de cumplimiento y pruebas sustantivas. El muestreo de atributos es la técnica mas adecuada para escoger una muestra de documentos fuentes para pruebas de cumplimiento.

El auditor puede realizar pruebas sustantivas o pruebas de doble propósito (pruebas sustantivas y de controles) por lo que en su proceso de diseño de pruebas de control deberá identificar para cada prueba la población de transacciones que ha sido sujeta a este control y el tipo de evidencia que va ha mostrar cumplimiento con el control.

2.6.1.2 Pruebas Sustantivas

El auditor debe identificar los procesos manuales y automáticos, que quiere verificar y escoger la técnica de auditoría más adecuada para realizar las pruebas. Las técnicas de auditoría incluyen:

- Lectura de los códigos de programas.
- Usar datos de prueba.
- Simulación en paralelo.
- Facilidad integrada de pruebas.

a. Lectura de los códigos de programas

- Verificar la autenticidad de los códigos fuente en relación al programa, sistema y/o aplicativo ejecutable.
- Identificar variables relacionadas con el proceso a verificar.
- Determinar el valor de las variables antes de ingresar al proceso a verificar.
- Realizar una prueba de escritorio.
- Incluir en los papeles de trabajo fotocopia del código en caso que el código tenga errores.

b. Usar Datos de Prueba

- Elaborar datos de prueba relacionadas con el proceso a verificar.
- Verificar el calculo de los resultados esperados.
- Ingresar los datos de prueba.
- Comparar los resultados obtenidos con los resultados esperados.

c. Simulación en Paralelo

- Obtener o elaborar programas específicos para realizar las pruebas en paralelo, verificar el funcionamiento de la simulación y documentar en los papeles de trabajo.
- Obtener las transacciones ingresadas al sistema, para someterlas a los programas de prueba.
- Comparar resultados obtenidos por los programas de prueba con los obtenidos por el sistema original.

d. Facilidad Integrada de Prueba

Esta prueba se realiza cuando los sistemas tienen mecanismos específicamente desarrollados que permitan identificar y diferenciar, lotes de datos de prueba, de manera tal que estos sigan todas las rutas de los datos originales pero que al final no afecten el estado de la información en las bases de datos, ni a los archivos maestros de los sistemas, ni que vayan a ser almacenados en archivos.

2.6.1.3 Prueba de Integridad de Datos

Este proceso consiste en identificar la información y documentación fuente que se utilizara para diseñar los procedimientos y procesos de pruebas de datos el mismo que consiste en:

- Identificar los archivos y las base de datos a verificar y obtener las definiciones de los mismos.
- Identificar los campos y relaciones de interés.
- Identificar las fuentes de información con la cual el auditor puede comparar el contenido de los archivos y base de datos.
- Diseñar los procesos de comparación con los documentos fuente u otras fuentes de información.
- Diseñar los procedimientos a efectuar, pudiendo usar los utilitarios de ACL o IDEA.

2.6.1.4 Auditabilidad de Sistemas

Todo sistema debe tener la capacidad de poder ser auditado, para lo cual el auditor deberá verificar que el sistema tenga las siguientes características:

- a. Contar con la documentación completa.
- b. Disponer de una biblioteca de pruebas.
- c. Disponer de Log del sistema.
- d. Contar con reportes de auditoría del sistema, para lo cual se deberá contar con utilitarios reportadores de base de datos para producir reportes de cruce de información.

Por lo tanto deberá verificarse que el sistema disponga de las características indicadas para facilitar su auditoría y en caso de no contar con ellos exigirá que se disponga su implementación, la cual puede ser considerada en el informe final.

Se deberá verificar que se hayan utilizado las técnicas adecuadas para cada etapa y sub-etapas del análisis, diseño, desarrollo, instalación, implantación y mantenimiento en la verificación y evaluación del Sistema, por lo cual para cada etapa se aplicarán las siguientes técnicas:

1 Análisis de Sistemas

- Entrevistas.
- Diagrama de Flujo de Datos (D.F.D.).
- Modelación de Datos.

- Diagrama de Estructura de Datos (D.E.D.).
- Historia de Vida de la Entidad (H.E.V.).
- Análisis de Costo-Beneficio (A.C.B.).
- Prototipo.

2. Diseño de Sistemas:

- Diseño Estructurado.
- Diagrama de Estructura de Cuadros.
- Optimización del Diseño Físico.
- Diseño de Pruebas.
- Prototipo.

3. Desarrollo de la Programación:

- Programación Estructurada.
- Pruebas Unitarias.
- Pruebas de Integración.
- Prueba del Sistema.

4. Instalación e Implantación de Sistemas:

- Capacitación.
- Creación de archivos iniciales.
- Proceso en paralelo.

5. Mantenimiento del Sistema

- Proceso de requerimientos.
- Áreas encargada del mantenimiento.
- Satisfacción del usuario que requiere el mantenimiento

2.6.2 Aplicación de Herramientas:

No basta con evaluar el sistema tomando conocimiento de su documentación y sosteniendo reuniones de revisión técnica con el personal involucrado, lo fundamental es que se demuestre la buena funcionalidad y confiabilidad del sistema por lo que hay que efectuar procesos de prueba simulando situaciones extremas de tal forma que se determine si el sistema responde a lo especificado y es confiable produciendo resultados correctos en los tiempos esperados. Es por eso que se deben realizar Benchmark o Pruebas del Sistema (procesos especiales) que permita realizar la evaluación y confiabilidad de los sistemas tales como:

2.6.2.1 Prueba Unitaria

Conjunto de pruebas que se realizan en una parte pequeña del programa con minuciosidad antes de integrarlo a un sistema más grande.

2.6.2.2 Prueba de Integración

Su objetivo es llevar a cabo pruebas para detectar errores asociados con la interacción de los módulos contenidos en su sistema. Construye una estructura de programa que este de acuerdo con lo que se dicte en el diseño.

2.6.2.3 Pruebas de Verificación

El objetivo es verificar el funcionamiento de los controles, la integridad de datos y el correcto funcionamiento de los recursos informáticos que fueron identificados en la etapa de revisión para obtener la evidencia necesaria que permita elaborar el informe.

Las actividades incluidas en esta etapa son la verificación en base al seguimiento del flujo de procedimientos y la aplicación de los controles, pruebas de cumplimiento, pruebas sustantivas, pruebas de archivos y base de datos, pruebas de sistemas de telecomunicación (incluye redes locales), lógica de programas, así como de la evaluación de la Gestión del Área de Sistemas.

Referente a la verificación de la calidad de los sistemas implementados tienen que ser tal que permitan una óptima operatividad del mismo, también debe ser verificado con el área usuaria que es responsable de operarlo y administrarlo; la información evaluada garantizará que:

- a. Cumpla con los requerimientos del usuario, establecido en la fase de Análisis y Diseño del Sistema.
- b. La secuencia de trabajo u operación del sistema, sea el mismo que el de proceso manual que se realiza en forma real.
- c. El sistema sea totalmente operado con la Guía del usuario o manual del usuario, asimismo ayudas permanentes que guíe al usuario.
- d. El tiempo de respuesta sea adecuado para el volumen real de datos.
- e. El consumo de recursos de cómputo sea razonable y esté dentro de lo previsto.
- f. Responda a todas las bifurcaciones posibles en la operación del sistema.
- g. La interfase-usuario sea adecuada y de fácil manejo y comprensión.
- h. Se disponga de todas las facilidades utilitarias de reorganización de archivos y copias de respaldo.
- i. Se disponga de procedimientos de respaldo ante caídas del sistema.

Antes de terminar el trabajo de campo el auditor del equipo debe revisar todos los papeles de trabajo para determinar:

- Si existe evidencia suficiente y competente para respaldar las conclusiones incluidas en los papeles de trabajo.
- Si la comisión de auditoría deberá realizar pruebas adicionales no incluidas en el programa de trabajo.
- Solamente deben pasar a la etapa de elaboración del informe cuando estén convencidos que tienen la evidencia necesaria, suficiente y competente para respaldar sus conclusiones.

Las actividades principales para la ejecución de la verificación son:

- 1 Verificación del flujo de datos y aplicación de controles.
- 2 Verificación de las pruebas de cumplimiento.
- 3 Verificación de las pruebas de integridad de datos.
- 4 Verificación de las pruebas de programas.
- 5 Verificación de la documentación del sistema.
- 6 Evaluación de la tecnología utilizada.

1. Verificación del flujo de datos de datos y Aplicación de Controles.

En base al diagrama de flujo de documentos que incluye el diagrama del sistema y la identificación de controles obtenidos de la entidad debe verificarse la autenticidad del mismo y si los controles mencionados existen.

Para realizar esta verificación debemos escoger las transacciones más sensibles y realizar el seguimiento de las mismas desde el inicio hasta el final del proceso comparando el sistema actual con la documentación. El auditor deberá recomendar que se actualice el diagrama del sistema y la identificación de controles cuando existan diferencias.

2. Verificación de Pruebas de Cumplimiento

Estas pruebas se realizan sobre los controles identificados en la etapa de revisión, donde el auditor deberá realizar las pruebas y analizar los resultados para determinar si los controles están funcionando de acuerdo con su diseño y si son confiables.

El auditor deberá documentar las debilidades que fueron encontradas en su análisis y evaluación de control interno. Estas debilidades pueden incluir controles que fueron diseñados pero que no están funcionando y puntos donde debe haber controles pero que no existen, deben existir los controles específicos de:

- Detección de errores.
- Prevención de acceso no autorizado y mal uso de la información y del equipo.
- Controles ambientales y seguridad.

3. Verificación de las pruebas de Integridad de Datos

El propósito de realizar pruebas de integridad de datos (prueba sustantiva) es verificar que los datos incluidos en archivos y/o bases de datos son confiables efectuando pruebas de existencia, exactitud y totalidad. Esta verificación incluye dos factores principales:

- La confiabilidad del contenido actual
- Los procesos de actualización.

LA CONFIABILIDAD DEL CONTENIDO ACTUAL

Para verificar el contenido actual de los archivos y/o las base de datos es necesario identificar una fuente de información a parte del medio magnético con el cual el auditor puede hacer comparaciones para verificar el contenido del medio. El auditor debe escoger una muestra de los registros y comparar los datos del registro con la fuente de información externa para verificar que la información contenida en el

archivo y/o base de datos es válida y que la entidad o transacción esta registrada. También el auditor debe escoger una muestra de transacciones o entidades en la fuente externa y comparar estas con los correspondientes registros en el archivo y/o base de datos para determinar si estas están completas.

LOS PROCESOS DE ACTUALIZACION

Para probar los procesos de actualización el auditor debe obtener dos copias de los archivos y/o bases de datos antes y después de la actualización y los datos que fueron usados para actualizarlos. El auditor debe escoger una muestra de las transacciones para probar el proceso de actualización. Usando los datos de la muestra junto con la copia de los archivos y/o bases de datos previa a la actualización el auditor deberá calcular los valores actualizados de los registros escogidos. El auditor posteriormente comparara sus cálculos con los datos de la copia posterior a la actualización para determinar si el proceso de actualización es adecuado. Esta prueba debe ser diseñada con las pruebas de programas (pruebas sustantivas) para poder efectuar las dos pruebas al mismo tiempo.

El archivo de sistemas también debe revisar los procedimientos de control de uso y backup de archivos y bases de datos para ver si son adecuados.

Existen paquetes como ACL e IDEA que son herramientas adecuadas para realizar pruebas de integridad de datos.

4. Verificación de las pruebas de Programas

Estas son pruebas sustantivas diseñadas para determinar si los procesos automáticos fueron diseñados e implementados correctamente y si las salidas de los programas son confiables. El auditor debe escoger los procedimientos que desea probar y la técnica que desea utilizar. Tomando en cuenta los procesos del sistema el auditor tiene que desarrollar datos de prueba o usar datos de entrada que se utilizaron en la gestión y determinar cual deberá ser la salida correcta del sistema con estos datos. Después de entrar los datos en el sistema el auditor debe comparar la salida actual del sistema con los resultados esperados para concluir si los procedimientos del sistema son adecuados.

También como pruebas básicas de programas el auditor puede comparar el tamaño (numero de bytes) del programa actual con el tamaño del programa después de su ultima modificación o auditoría para buscar evidencia de modificaciones no autorizadas. El auditor también puede usar un editor para buscar por números de cuentas y/o líneas específicas (cuentas de programadores o terceros u otros valores constantes en programas) para intentar encontrar código no autorizado.

5. Verificación de la documentación del Sistema

La documentación deberá ser revisada permanentemente en cada etapa de evaluación, siendo recomendable que se revise antes de la auditoría.

Deberá llevarse un registro de control de la documentación generada, para efectos de seguimiento permanente y control posterior.

Deberá contarse documentadamente con actas u otro documento donde se tenga la conformidad del usuario de la documentación que éste deba utilizar.

Si el control es realizado posteriormente, deberá verificarse la existencia de toda la documentación y la aprobación del usuario.

Con la documentación de sistemas generada, se debe verificar que todas las etapas y sub-etapas de la Metodología de Requerimiento, Análisis, Diseño, Programación, Prueba, Instalación e Implantación de Sistemas se hayan ejecutado con resultados satisfactorios.

6. Evaluación de la Tecnología Utilizada

El auditor verificara la tecnología utilizada sea la más adecuada a los fines del sistema, y permita una vida útil satisfactoria para la inversión realizada. Por lo que verificara lo siguiente:

- Equipos.
- Sistema de Red.
- Sistema de Base de Datos.
- Sistema de Comunicaciones.
- Lenguaje de Programación.

Es conveniente indicar que en algunas Organizaciones tienen toda su plataforma de Hardware y Software que utilizan como estándar para la Institución, quedando en este caso tratar de aprovecharla al máximo.

También, existen organizaciones en la que se dan soluciones departamentalizadas con interfaces entre ellas, manteniendo cierta independencia entre si.

Equipos:

Se deberá verificar que los equipos sean los adecuados, de acuerdo al tipo de sistema que se estén utilizando. Si la aplicación es monousuaria, se requerirá un equipo que tenga independencia de operación, debiendo contar individualmente con el equipo adecuado que soporte todo el procesamiento.

En caso de que el sistema sea multiusuario, deben utilizarse equipos terminales conectados a un servidor, debiendo estar balanceados adecuadamente los recursos entre ambos, de tal forma de contar con una performance aceptable.

Sistema de Red:

Dependiendo del tipo de Sistema, se deberá utilizar el tipo de plataforma de Red que más convenga. Si el sistema es cerrado y netamente operativo con un criterio de procesamiento centralizado, pueden utilizarse sistemas orientados a la centralización y si el sistema es de filosofía abierta y descentralizada, se deben utilizar redes de este tipo.

Sistema de Base de Datos:

En función a las necesidades del sistema se debe utilizar la plataforma necesaria de Base de Datos. Para aplicaciones sencillas e independientes, se utiliza el manejador de base de datos del lenguaje. Sin embargo, para aplicaciones corporativas, se utilizan manejadores de base de datos relacionales de nivel, así como para aplicaciones de tipo cliente-servidor .

Sistema de Comunicaciones:

Este es un factor importante a evaluar en función a la naturaleza del sistema. Muchas veces el sistema debe instalarse en una topología de comunicaciones pre-establecida y hay que tratar de aprovecharla al máximo. Sin embargo, si el diseño de las comunicaciones pudiera estar correlacionado con el sistema, permitiría un mejor desempeño de las mismas.

Lenguaje de Programación

Se debe evaluar si el lenguaje a utilizar o ya utilizado es el más conveniente, dependiendo de las necesidades de eficiencia y facilidad de desarrollo y explotación, por lo que deben evaluarse los siguientes factores:

- Ambientes gráficos; Tiempos de procesamiento y respuesta.
- Facilidades en tiempos de programación y mantenimiento de sistemas.

Rapidez en el desarrollo de sistemas a través de generadores de programas.

2.6.2.4 Prueba de carga máxima

Determinar si el sistema maneja el volumen de actividades que ocurren cuando este se encuentra en el punto máximo de demandas de procesamiento (Ejemplo todos los terminales se encuentran activadas y operando).

2.6.2.5 Prueba de almacenamiento

Determinar la capacidad del sistema para almacenar datos de transacciones en un disco o en otros archivos (Ejemplo: verificar datos de documentación que el sistema almacenara 10 mil registros de 383 bytes de longitud en un solo disco flexible de baja densidad).

2.6.2.6 Prueba de tiempo de ejecución

Determinar el tiempo que utiliza el sistema para el procesamiento de datos de transacciones. (Ejemplo: Tiempo de respuesta a las consultas cuando el sistema se encuentra totalmente cargado con datos operativos).

2.6.2.7 Pruebas de Seguridad

Determinar mecanismos de protección incorporados en el sistema para evitar la penetración impropia (Ejemplo: Ingresar al sistema con todas las técnicas posibles para dicho efecto).

2.6.2.8 Pruebas de Resistencia

Se diseñan para que los programas enfrenten a situaciones anormales (Ejemplo: Interrupciones, frecuencias exageradas de ingreso de datos, de búsquedas, etc.).

2.6.2.9 Pruebas de Recuperación

Determinar la posibilidad del usuario para recuperar datos o para iniciar el sistema nuevamente después de un error.

2.6.2.10 Pruebas de Procedimientos

Determinar la claridad de la documentación en operación y uso del sistema logrando que los usuarios hagan exactamente lo que los manuales indican.

2.6.2.11 Pruebas de Factores Humanos

Determinar la manera en que los usuarios utilizaran el sistema cuando procesen datos (Ejemplo: Las actividades del usuario cuando no existe una respuesta inmediata a una consulta – pantallas en blanco durante un proceso).

2.6.3 Técnicas de Auditoría de Sistemas en Funcionamiento:

A Continuación exponemos las técnicas que comúnmente se utilizan para evaluar los sistemas en funcionamiento, siguiendo los lineamientos del Stanford Research Institute (SRI), según una investigación que desarrollo sobre la materia, por considerar que se trata de un trabajo que cubre, en forma completa, todo el campo,

objeto de auditoría, en sistemas o aplicaciones en funcionamiento; estas técnicas se dividen en:

2.6.3.1 Técnicas Administrativas.

2.6.3.2 Técnicas para probar controles de sistemas en funcionamiento.

2.6.3.3 Técnicas de selección y monitoreo transacciones.

2.6.3.4 Técnicas para el examen de archivos.

2.6.3.5 Técnicas para examinar programas aplicativos.

2.6.3.1 Técnicas Administrativas

Las técnicas administrativas para efectos de auditoría de sistemas en funcionamiento se dividen en dos categorías:

1.- Técnicas para establecer el orden de prioridades en el auditaje de aplicaciones, en el funcionamiento:

Selección de áreas de auditoría.

Es una técnica que facilita la determinación de las áreas auditables, en orden prioritario, a partir de la colección y evaluación estadística de las operaciones de la entidad auditada, en forma periódica, con el objeto de extraer información clave como por el ejemplo, un alto nivel de cuentas incorporables, devoluciones de ventas en exceso, obsolescencia de inventarios y otros.

Esta técnica es recomendable, especialmente, para empresas con múltiples localizaciones o sucursales y con un alto grado de integración de sus sistemas aplicativos.

Simulación – modelaje

Esta técnica es similar a la de selección de áreas de auditoría, excepto que se utiliza básicamente para evaluar el desempeño financiero en forma periódica. Compara estimaciones de valores esperados con valores actuales con el objeto de identificar desfases significativos lógicamente relacionados, en materia financiera.

Sistema de Puntajes (scoring)

Esta es una técnica de evaluación manual, de las aplicaciones computarizadas, con el objeto de establecer prioridades para efectos de auditoría sobre la base de análisis de riesgos.

La técnica consiste en asignar valores numéricos a las características claves de las aplicaciones en funcionamiento para detectar las áreas de mayor interés para auditoría.

Entre otros, los factores que normalmente se tienen en cuenta para decidir el proceso de selección son los siguientes:

- A. Valor de los activos sometidos a control.
- B. Vulnerabilidad al fraude.

- C. Nivel de modificación al sistema y/o al programa.
- D. Grado de participación de la auditoría en el desarrollo de nuevas aplicaciones.
- E. Software utilizado, en general.
- F. Recursos de hardware utilizados.
- G. Regularidad y uso de los reportes generados por el sistema.

El auditor ideará los criterios para la asignación de la ponderación que le corresponda a cada factor y clasificar los resultados y las aplicaciones correspondientes, teniendo en cuenta obviamente, la intensidad de los riesgos potenciales.

2.- Técnicas para operacionalizar la función de auditoría

a. Software de auditoría multisitio.

Es una técnica aplicable a organizaciones que tienen centros de PED regionales o remotos y un STAFF centralizado para el desarrollo de sistemas y de programación de computadores. Esta técnica implica la preparación y distribución centralizada de software de AUDITORIA para ser utilizado, después, en forma descentralizada, en las diferentes dependencias regionales o remotas de la organización, de donde deriva la denominación de multisitio.

Esta técnica administrativa de auditoría de sistemas es de amplia aplicación en ambientes de procesamiento distribuido.

b. Centros de competencia.

La técnica denominada “CENTROS DE COMPETENCIA” supone un CENTRO DE COMPUTO responsable de la ejecución centralizada de los programas de auditoría de sistemas.

El procedimiento operativo consiste en que los CENTRO DE COMPETENCIA reciben los archivos de datos, procedentes de localizaciones remotas, les aplican los programas de auditoría pertinentes y después, distribuyen los informes resultantes a los auditores regionales para su análisis, evaluación y decisiones consecuentes. Como puede observarse, esta técnica funciona a la inversa del concepto de AUDITORIA MULTISITIO, en cuanto a la aplicación del software de AUDITORIA.

2.6.3.2 Técnicas para probar controles de sistemas en funcionamiento

Las técnicas de auditoría de sistemas para probar controles en programas de aplicación, se orientan básicamente en verificar los cálculos en aplicaciones complejas, comprobada la exactitud del procesamiento en forma global y específica y verificar el cumplimiento de los controles pre- establecidos de acuerdo al manual correspondiente.

1. Método de Datos de Prueba

La técnica de DATOS DE PRUEBA, comúnmente llamada “ lotes de prueba “ (test decks), consiste en un conjunto de datos de entrada que presentan al computador variedad de transacciones para verificar a través del procesamiento, como medio para detectar resultados no validos.

Los datos de prueba deseables deben de representar la aplicación que se examina con toda las posibles combinaciones de transacciones, situaciones de archivo maestro, valores de lógica y procesamiento que podrían encontrarse durante las operaciones reales para que la verificación de los datos sea factible debe de contarse con documentación de la publicación confiable. Esto es que incluya detallada y completa sobre los formatos de transacciones de formatos de archivos maestros, las condiciones de procesamiento y controles.

Los resultados de los DATOS DE PRUEBA, arrojados por el programa examinado se compran con los resultados predeterminados calculados manualmente para detectar inconsciencia de orden lógico o de exactitud de procesamiento, cuando los datos de prueba son voluminosos sé acostumbrar reparar rutinas que tiene como objetivo evitar los procesos manuales los cuales resulta dispendiosos.

La técnica de DATOS DE PRUEBA, es normalmente utilizada en la fase de prueba del programa por los analistas – programadores antes de enviar los programas a producción

El archivo maestro puede ser:

1. Una copia de archivo de producción.
2. Un archivo con datos simulados creado por el auditor.

Los programas utilizados para correr los datos de prueba deben de ser los mismos que se encuentran en Producción y que se utilizan para procesar los movimientos corrientes.

2. Evaluación del Sistema de caso base (BCSE)

La técnica de evaluación del sistema de caso base, es conceptualmente similar al método de datos de prueba, ambas técnicas se ocupan de probar la lógica de los programas y la precisión de los cálculos, vía datos de prueba pero la BCSE es más completa y requiere un alto grado de cooperación entre los usuarios auditores y personal del sistema para su ejecución, la técnica BCSE se utiliza especialmente para validar los sistemas antes de entrar a producción, pero también se utiliza normalmente por los auditores para examinar aplicaciones en funcionamiento.

El paquete de datos para la prueba de BCSE es preparado por los usuarios en colaboración con los auditores y personal de sistema y no se abandona como en el método de datos de prueba sino en el se actualiza o mantiene permanentemente de acuerdo la evolución de sistemas.

3. Operación Paralela

La operación paralela es una técnica muy utilizada para verificar la exactitud de los sistemas nuevos o revisados, consiste en el proceso de mismos datos reales con procedimiento actuales y nuevos para luego comparar los resultados y detectar inconsistencias.

Los programas y procedimientos actuales no se abandonara sino asta cuando los nuevos arrojen los resultados esperados.

Cuando se tiene un sistema manual se diseña un sistema por computador es necesario llevarlo en PARALELO hasta cuando los resultados del sistema por computadora coincidan con los resultados del sistema manual. En ese momento se deja la OPERACION PARALELA esto es, que se abandona el sistema antiguo y se sigue con el nuevo.

4. Facilidad de Prueba Integrada

La facilidad de prueba integrada es una técnica para procesar datos de prueba a través de sistemas de aplicación. con los datos reales esta técnica permite examinar el procesamiento de una aplicación en su ambiente normal de producción.

Se utiliza normalmente una ENTIDAD FICTICA (mini compañía) establecida, para fines de auditoria dentro de la estructurar de la aplicación.

El auditor procesa transacciones de prueba para la entidad ficticia, junto con las transacciones reales de producción y a esto se debe que la técnica se llama INTEGRADA.

Además esta técnica se caracteriza por lo siguiente:

- Los registros maestros, utilizados por el AUDITOR, residen en los mismos archivos en donde residen los registros reales de producción.
- Los datos de prueba devengan de afectar únicamente la entidad ficticia. Se requiere un método que evite afectar los informes reales con los datos de prueba, eliminándolos adecuada y oportunamente.

Los resultados de los datos de prueba, procesados mediante la técnica de facilidad de prueba integrada, deben compararse con los resultados precalculados de los mismos datos para examinar la lógica de los programas y el nivel de precisión del procesamiento.

Como puede observarse la técnica denominada “facilidad de prueba integrada” es un refinamiento del enfoque de los datos de prueba.

5. Simulación en Paralelo

La técnica de simulación en paralelo, consiste en preparar una aplicación computarizada, por separado, que efectúe las mismas funciones que los programas de aplicación reales utilizados para el procesamiento diario u otros procedimientos periódicos. Los programas de simulación leen los mismos datos de entrada con los

programas de aplicación, utilizan los mismos archivos y tratan de producir los mismos resultados. Dichos resultados se comparan con los producidos por los programas reales a fin de establecer si son iguales o hay discrepancia.

Las simulaciones en paralelo reciben su nombre del hecho de que es el que AUDITOR puede crear un nuevo juego de programas de aplicación que procesan información en paralelo con los programas de producción oficiales.

La técnica de simulación el paralelo se diferencia de las técnicas de DATOS DE PRUEBA Y DE FACILIDAD DE PRUEBA INTEGRAL, en que procesa datos REALES a través de programas simulados y aquellas que procesan datos simulados a través de programas REALES.

Esta técnica permite verificar y evaluar básicamente las siguientes funciones. :

- Procedimiento de control y de validación de entrada.
- Cálculos y lógica de procesamiento.
- Lógica de actualización de archivos maestros.
- Controles y procedimiento de balanceo.

2.6.3.3 Técnicas para seleccionar y monitorear transacciones

Las técnicas usadas para seleccionar y capturar datos en los procesos corrientes de PED, para luego someterlos a evaluación por parte de AUDITORIO, son básicamente: Selección de transacción de entrada, módulos de auditorio incluido en

los programas ampliativos tipo SCARF/ SARF y registros extendidos. Los criterios de selección son generalmente parámetros controlados.

Hago un muestreo y condiciones de error. Esta técnicas es utilizada con mayor frecuencia para desarrollar programas de auditorio de cumplimiento.

1. Selección de Transacciones de entrada

Es una técnica que se ejecuta con software de AUDITORIA, independientemente del software aplicativo. Consiste en seleccionara y separar datos d e entrada que asen parte de las aplicaciones corrientes mediante parámetros diseñados por el auditor, con base en su propio criterio. Las muestras de transacciones separadas son sometidas a examen detallado por parte del personal experto de auditoria con base en los objetivos pre- establecido.

Es una técnica relativamente fácil de aplicar y no requiere modificación de software de sistema aplicativo no se presenta riesgos de alteración de la información real generada por el sistema en producción debido a que la técnica opera en forma independiente de los programas ampliativos.

2. Archivo de revisión de auditoria como control del sistema (SCARF)

La técnica de “archivo de revisión de auditoria como control del sistema” (SCARF), consiste en la incorporación del modulo de auditoria en los programas aplicativos para que ejecuten funciones de supervisión o monitoreo de transacciones

en forma permanentemente este procedimiento usa software de auditoria para marcar y seleccionar transacciones de entrada y transacciones generado, dentro de sistema de aplicaciones, durante el procesamiento. Tales sub-rutinas son integradas, como huéspedes, dentro de los programas aplicativos.

Las actividades de supervisión o monitoreo, muestreo y reporte de excepción son todos controlados por parámetros debidamente definidos por auditoria los pasos seguidos para implantar esta técnica son generalmente los siguientes:

- El auditor precisa sus requerimientos al personal de desarrollo de sistemas, en la etapa de diseño de nuevas aplicaciones.
- Los anglicistas – programadores prepararan las rutinas y las implantan dentro del programa de aplicación.
- Los controles especificados por auditoria, funcionan simultáneamente con el programa de producción y las excepciones van siendo registrados en un archivo dirigido a auditoria el cual es revisar manualmente o con ayuda del computador.

Esta técnica es bastante aconsejable para a ambientes de procesamiento ON LINE, en sus diferentes modalidades.

3. Archivo de revisión de auditoría por muestreo (SARF)

La técnica denominada “ARCHIVO DE REVISION DE AUDITORIA DE MUESTREO SARF”. Es similar a la técnica SCARF, excepto en que su contenido se selecciona al azar, el objetivo de esta técnica es obtener un archivo representativo para e efectos de análisis de AUDITORIA.

La técnica SARF es particularmente es apropiado para los auditores externos quienes necesitan examinar los archivos y las transacciones en forma aleatoria, apiladores en el MUESTREO estadístico.

Los pasos que se siguen para implantar la técnica SARF son básicamente los mismos utilizados para la técnica SCARF, veámoslos:

- El auditor de fine sus requerimientos y los comunica al personal de desarrollo de sistemas, en la etapa de diseño de nuevas aplicaciones.
- Los analistas – programadores preparan los módulos de auditoria correspondientes y los incluyen dentro de los programas de producción.
- Una vez que se ha puesto a funcionar el nuevo sistema, la rutina de selección al azar origina los registros que han de ser llevados a un archivo para análisis de auditoria.

La diferencia entre la técnica SCARF y SARF, esta en que la primera, los criterios de selección se incluyen en el modulo de auditoria y en la segunda los parámetros se especifican al tiempo de la corrida del programa.

4. Registros extendidos.

La técnica de los registros extendidos permite recoger o seleccionar por medio de rutinas especiales, todo los datos significativos que han afectado una transacción individual.

Funciona acumulando en un único registro, los datos originados en un mismo periodo, correspondientes a una transacción individual completa.

Esta técnica es instalada por el personal de análisis y programación en momento de preparar software aplicativo y constituye un una pista completa de auditoria.

El registro extendido tiene la propiedad de consolidar el procesamiento de varios periodos de años en forma histórica evitando de esta manera la perdida de pistas de auditoria especialmente como consecuencia de la reorganización anual de los archivos maestros.

2.6.3.4 Técnicas para el examen de archivos

Esta técnica para el examen de archivos, vamos a estudiar el software de auditoria que tiene origen básicamente en las siguientes fuentes:

1. Programas generalizados de Auditoría.

Los programas de auditoría generalizados, constituyen una técnica muy importante para examinar los archivos de las empresas, cuyos procesos se llevan por computador.

Normalmente los auditores encuentran que el trabajo de examinar los archivos de las organizaciones no varía notablemente de una entidad a otra. La esencia del examen se concreta en actividades, tales, como: clasificar, resumir, extraer, insertar, mezclar (intercalar), comparar calcular, selecciona, evaluar y otras actividades similares.

Sin embargo en la práctica, se han encontrados algunas dificultades para aplicar software generalizado de auditoría, como por ejemplo:

- Diversidad de marca de computadora.
- Complejidad creciente de configuración de equipos.
- Diferentes lenguas de programación.

No obstante, las dificultades anteriores el avance vigoroso.

Han tenido los lenguajes de alto nivel hacen pensar que un corto plazo vamos a tener software de auditoría.

La mayoría del software generalizado de auditoria se encuentran dentro de las siguientes clases.

- Paquetes diseñados para actividades específicas tales como las cosas de valor y/o entidades financieras en general.
- Paquetes utilizan un lenguaje de auditoria él mas alto nivel en los cuales los programas de auditoria se escriben para los archivos específicos de datos que van a ser examinados paquetes en los cuales los programas son estandarizados y los archivos de datos sometidos a examen se modifican y adoptan de tal manera el programa pueda utilizarse con dichos archivos.

La tercera modalidad de los paquetes esta diseñada de manera que pueda utilizarse en diferentes aplicaciones.

Los programas estandarizados de auditoria pueden adaptarse normalmente a aplicaciones que se están procesando en equipo grandes y medianos. En el caso de equipos pequeños no compatibles es necesario escribir programas a medida.

A continuación exponemos algunos paquetes de auditoria generalizado de uso frecuente en nuestro medio.

2.6.3.5 Técnicas para examinar programas aplicativos

Se entiende por programas aplicativos aquellos que siendo estandarizados y/o a la medida tienen como objetivo la solución de problema por computadora.

1. SNAPSHOT (Imagen Instantánea).
2. MAPPING (Mapeo).
3. TRACING (Rastreo).
4. CONTROL FLOWCHARTING (Flujograma de Control).
5. COMPARACION DE CODIGOS.
6. CONTROL DE BYTES.
7. REPROCESO CONTROLADO.
8. ANALISIS DE LA LOGICA DE LOS PROGRAMAS.

1. SNAPSHOT (Imagen Instantánea)

La técnica SNAPSHOT implica un conjunto de instrucciones que reconocen y permiten registrar el flujo de transacciones señaladas, durante todo el camino lógico seguido por dichas transacciones, dentro de los programas de aplicación.

Pasos:

- a. El auditor proporciona sus requerimientos detallados, a los analistas-programadores, durante el desarrollo del programa aplicativo.
- b. Los analistas-programadores implantan las rutinas para obtener pistas de auditoría, a nivel selectivo, en el momento de los procesos normales, de producción.
- c. Después de montada la nueva aplicación, puede añadirse una clave especial a los datos de entrada, sin afectar los resultados finales de las transacciones seleccionadas.

- d. Durante el procesamiento de las transacciones, con clave especial, se producen reportes en puntos predeterminados, con el objeto de revelar el impacto que la transacción “marcada” tiene sobre los registros maestros de la aplicación.
- e. El auditor recibe la documentación de las pistas de transacciones y desarrolla su proceso de análisis correspondiente, de acuerdo con sus objetivos de auditoría predefinidos.

2. MAPPING (Mapeo)

El MAPPING es una técnica ejecutada por una herramienta de medición de software que analiza un programa de computador, durante su ejecución, para determinar si son utilizadas todas las instrucciones del programa. Cuenta el número de veces que es ejecutada instrucción y mide el tiempo de CPU consumido por cada instrucción.

Además, el resultado expresa lo siguiente:

- Indica una lista de cualquier segmento del programa no utilizado.
- Detalla una lista de pasos que consumieron mayor tiempo de CPU.
- Muestra una lista del programa fuente detallando el número de veces que cada instrucción fue ejecutada.

Esta técnica es frecuentemente utilizada en auditoría para identificar las rutinas del programa autorizadas.

3. TRACING (Rastreo)

La técnica de TRACING puede definirse como una opción de los lenguajes de programación que permite identificar y mostrar las instrucciones que fueron ejecutadas y en qué secuencia. Le facilita al auditor la ejecución de un recorrido electrónico a través de procesamiento normal de aplicaciones.

4. CONTROL FLOWCHARTING (Flujograma de Control)

Facilitan la tarea de verificar si los controles están operando, en la forma como fueron establecidos y documentados.

Normalmente, se diseñan en primer lugar, macrodiagramas, los cuales tienen como objetivo mostrar una imagen total de los sistemas de procesamiento y de control. Después se diseñan diagramas detallados con el objeto de:

- A. Identificar y rastrear los controles sobre los diferentes documentos generadores de datos.
- B. Evaluar la segregación funcional.
- C. Detectar las deficiencias y excepciones en materia de control y en general de tipo operacional.

5. COMPARACION DE CODIGOS

La técnica de comparación de códigos se usa para examinar dos versiones consecutivas de un programa, con el objeto de verificar si se están siguiendo

correctamente los procedimientos de mantenimiento y cambio de programas y de librerías de programas.

6. CONTROL DE BYTES

La técnica de CONTROL DE BYTES consiste en someter a verificación de número de BYTES los programas aplicativos para detectar, por éste medio, modificaciones no autorizadas. En un ambiente de rigurosa segregación funcional, ésta técnica ofrece un alto grado de confiabilidad en materia de integridad de los programas y de inviolabilidad de sus contenidos. Tendrían que eliminarse instrucciones con determinado número de bits e incluir instrucciones fraudulentas exactamente con el mismo número de bits, pero sin alterar los procesos funcionales, para evitar ser descubierto fácilmente, lo cual no es precisamente corriente, cuando exista un consolidado sistema de control interno informático.

7. REPROCESO CONTROLADO

La técnica puede aplicarse volviendo a procesar todos los datos de un movimiento o sencillamente reprocesando un grupo de transacciones a criterio del auditor.

Para evitar la duplicidad del registro de los datos, se utilizan copias de los archivos de las aplicaciones correspondientes. De lo contrario habría que hacer la reversión del reproceso pero esto resulta más riesgoso.

8. ANALISIS DE LA LOGICA DE LOS PROGRAMAS

Seguramente, una de las técnicas de auditoría de sistemas, que puede utilizar un auditor para quedar convencido de que todos los controles necesarios existen en un programa de computador, que los controles necesarios existen en un programa de computador, que los controles se encuentran operando en forma efectiva y que el programa se encuentra procesando datos de acuerdo con las políticas establecidas, consiste en revisar la lógica del programa, como se encuentra contenida en la documentación oficial del programa.

La documentación del programa, para efectos de la revisión de la lógica, puede consistir en los siguientes componentes:

- Una narración descriptiva y detallada del programa.
- El diagrama de lógica detallado de los programas.
- Los listados de los programas.

2.7 Elaboración del Informe Final

El objetivo de la elaboración del informe final, de la comisión de auditoría es presentar las observaciones, conclusiones y recomendaciones, expresadas en juicios fundamentados (papeles de trabajo) como consecuencia del análisis de las evidencias obtenidas durante la etapa de control.

Antes de preparar el informe los auditores revisaran la evidencia obtenida para asegurar que es suficiente, competente y que respalde su informe. Asimismo el estilo de escritura de la estructura del informe deberá centrarse en los siguientes aspectos:

- Anticipe preguntas.
- Problema, causa y efecto.
- Cuantifique hechos.
- Evite lenguaje técnico, inflamatorio.
- Evite ambigüedades.
- Tiempo pasado.

2.7.1 Estructura del Informe Final de Auditoría

Al finalizar el examen de control, la comisión de auditoría deberá elaborar un informe en el cual expondrá apropiadamente los resultados del examen, señalando que se realizó de acuerdo a las normas, procedimientos de auditoría, plan de auditoría y de los objetivos de la Institución, siendo el contenido del informe el siguiente:

2.7.1.1 Introducción del Informe Final.

2.7.1.2 Conclusiones.

2.7.1.3 Observaciones.

2.7.1.4 Recomendaciones.

2.7.1.5 Firma del informe.

2.7.1.6 Anexos.

2.7.1.1 Introducción del Informe Final

Comprenderá la información general concerniente al examen y a la entidad examinada.

A. Información relativa al examen

1. Motivo del Examen

Estará referida a las causas que originaron el examen, así como la referencia al documento de acreditación de la comisión de auditoría, debiendo exponerse las razones por las cuales se llevo a cabo la auditoría.

2. Naturaleza y Objetivos

Esta referido a lo que espera lograrse como resultado del examen. Al exponerlos se darán a conocer los límites de la auditoría, a fin de evitar interpretaciones erróneas en los casos en que los objetivos hayan sido particularmente limitados o puntales sobre determinados aspectos de la gestión.

3. Alcance

Deberá indicarse claramente la cobertura y profundidad del trabajo que se haya realizado para cumplir los objetivos de la auditoría,

precisándose el período examinado, el ámbito geográfico donde se haya practicado la auditoría y las áreas materia del examen.

Asimismo se dejara constancia que el trabajo se realizo de acuerdo con las normas y procedimientos de auditoría.

4. Comunicación de Observaciones

Se dará a conocer el cumplimiento de la comunicación de observaciones efectuada a los funcionarios de la entidad comprendidos en las mismas.

5. Limitaciones

Especificar los hechos que han limitado el alcance ha la ejecución del proceso de auditoría, las mismas que se pondrán de conocimiento de ser el caso.

B. Información relativa a la Entidad Examinada

1. Antecedentes y Base Legal

Se deberá hacer una breve referencia en torno a la creación de la entidad, su estructura organizativa, las principales actividades que desarrolla y al área examinada.

En la base legal se precisará la referencia a las disposiciones legales que la regulan.

2. Relación a las personas comprendidas en las observaciones

Está referido al personal de la entidad auditada comprendida en las observaciones, el cual se consignara en un anexo del informe, con indicación de nombres y apellidos, cargo, período de gestión, condición laboral y dirección domiciliaria.

3. Posición financiera, económica y presupuestaria

Teniendo en cuenta el tipo de examen que se realice, a criterio del auditor, se incluirán el balance general, estado de pérdidas y ganancias, balance de ejecución presupuestal u otros, según corresponda.

2.7.1.2 Conclusiones

Las conclusiones estarán referidas a la evaluación de los resultados de la entidad examinada, en cuanto al logro de los objetivos, metas y programas, así como a la utilización de los recursos informáticos de la entidad, en términos de economía, eficiencia y eficacia.

Asimismo el auditor deberá expresar sus conclusiones, que son juicios de carácter profesional basados en las observaciones resultantes del examen efectuado.

2.7.1.3 Observaciones

Es toda información que a juicio de la comisión de auditoría permita conocer hechos o circunstancias que incidan significativamente en:

- a. Inefectividad en el logro de objetivos y metas.
- b. Ineficiencia en las operaciones.
- c. Desperdicio de los recursos.
- d. Incumplimiento de leyes, reglamentos o políticas internas.

Los aspectos principales que deben tenerse en cuenta al redactar las observaciones serán:

- Las observaciones estarán referidas a asuntos significativos e incluirán información suficiente y competente relacionada con los resultados de la evaluación.
- Deberá incluir la información necesaria respecto a los antecedentes a fin de facilitar la comprensión de las observaciones.
- El termino observación esta referido a cualquier situación deficiente y relevante que se determine de la aplicación de procedimientos de auditoría y estará estructurada de acuerdo con los atributos: Condición, criterio, causa y efecto. Asimismo deberá redactarse en forma narrativa teniendo en cuenta para su presentación los atributos mencionados:

a. Sumilla

Es el título que se pondrá en el hecho observado.

b. Condición

Descripción de la situación irregular o deficiencia hallada, cuyo grado de desviación debe ser demostrada.

c. Criterio

Son las normas transgredidas de carácter legal, operativo o de control que regulan el accionar de la entidad examinada. El desarrollo del criterio en la presentación de la observación debe citar específicamente la normativa pertinente y el texto aplicable de la misma.

d. Causa

Es la razón fundamental por la cual ocurrió la condición o el motivo por el que no se cumplió el criterio o norma. Su identificación requiere de la habilidad y juicio profesional del auditor y es necesaria para el desarrollo de una recomendación constructiva que prevenga la recurrencia de la condición.

e. Efecto

Es la consecuencia real o potencial, cuantitativa o cualitativa, que ocasiona el hallazgo, indispensable para establecer su importancia y

recomendar a la Administración que tome las acciones requeridas para corregir la condición. Siempre y cuando sea posible, el auditor debe revelar en su informe la cualificación del efecto.

- Al término del desarrollo de cada observación, se indicaran de modo sucinto los descargos que presenten las personas comprendidas en la misma, así como la opinión del auditor después de evaluar los hechos observados y los descargos recibidos.
- Si durante el examen el auditor aprecia logros notables en la entidad auditada y que tengan relación con el alcance y objetivos de la auditoría, a su juicio podrá decidir su inclusión en los comentarios del informe.
- Tratándose de la existencia de posibles delitos el auditor debe deslindar y determinar el tipo de responsabilidad que corresponda a los presuntos implicados, contando para ello con una adecuada coordinación con la asesoría legal.

2.7.1.4 Recomendaciones

Las recomendaciones constituyen las medidas sugeridas a la administración de la entidad examinada orientadas a promover la superación de las observaciones o hallazgos emergentes de la evaluación de la gestión. Las recomendaciones serán dirigidas a los funcionarios que tengan competencia para disponer su aplicación.

El informe debe contener recomendaciones constructivas que, fundamentadas en los hallazgos y conclusiones correspondientes, propicien la adopción de correctivos que posibiliten mejorar significativamente la gestión y/o desempeño de los funcionarios y servidores públicos, con énfasis en el logro de los objetivos, metas y programas de la entidad auditada dentro de los parámetros de economía, eficiencia y eficacia.

Las recomendaciones presentaran los aspectos siguientes:

- a. Estar encaminadas a superar las causas de los problemas observados.
- b. Sean factibles de implantar y que su costo corresponda a los beneficios esperados.
- c. Deben contener la descripción de cursos de acción para optimizar el cumplimiento de metas y objetivos.
- d. Precisar las medidas necesarias para la acción correctiva, aplicando criterios de oportunidad, de acuerdo a la naturaleza de las observaciones.
- e. Que se cumplan las leyes y reglamentos aplicables y se mejoren los controles internos.

Se deberán incluir las recomendaciones significativas determinadas en auditorías anteriores que no se hayan corregido y estén relacionadas con los objetivos del examen.

2.7.1.5 Firma del Informe

El informe deberá ser firmado por Jefe de Comisión y el Supervisor de la Comisión y aprobación del Gerente de Línea de la Inspectoría General y del Inspector General. De ameritar el informe también será suscrito por el asesor legal y otro profesional y/o especialista que en el examen se solicite.

2.7.1.6 Anexos

Los anexos se utilizaran para complementar o ampliar información que permita el máximo de concisión y claridad en el informe.

Pueden estar referidos, entre otros aspectos, a los fundamentos de los descargos presentados por las personas comprendidas en los hechos observados, a los informes técnicos y legales, según la naturaleza de los hallazgos.

CAPITULO III

APLICACIÓN DE LA METODOLOGÍA DE ANÁLISIS DE RIESGOS

3.1 ETAPA 1: Diseño de Cuestionarios

3.1.1 Encuesta a Usuarios

La entrevista se deberá llevar a cabo para comprobar datos proporcionados y la situación de la dependencia en el departamento de Sistemas de Información.

Su objeto es conocer la opinión que tienen los usuarios sobre los servicios proporcionados, así como la difusión de las aplicaciones de la computadora y de los sistemas en operación.

Las entrevistas se deberán hacer, en caso de ser posible, a todos los usuarios o bien en forma aleatoria a algunos de los usuarios, tanto de los más importantes como

de los de menor importancia, en cuanto al uso del equipo.

Desde el punto de vista del usuario los sistemas deben:

- Cumplir con los requerimientos totales del usuario.
- Cubrir todos los controles necesarios.
- No exceder las estimaciones del presupuesto inicial.
- Serán fácilmente modificables.

Para que un sistema cumpla con los requerimientos del usuario, se necesita una comunicación completa entre usuarios y responsable del desarrollo del sistema.

En esta misma etapa debió haberse definido la calidad de la información que será procesada por la computadora, estableciéndose los riesgos de la misma y la forma de minimizarlos. Para ello se debieron definir los controles adecuados, estableciéndose además los niveles de acceso a la información, es decir, quién tiene privilegios de consulta, modificar o incluso borrar información.

Esta etapa habrá de ser cuidadosamente verificada por el auditor interno especialista en sistemas y por el auditor en informática, para comprobar que se logro una adecuada comprensión de los requerimientos del usuario y un control satisfactorio de información.

Para verificar si los servicios que se proporcionan a los usuarios son los requeridos y se están proporcionando en forma adecuada, cuando menos será preciso considerar la siguiente información.

- Descripción de los servicios prestados.
- Criterios de evaluación que utilizan los usuarios para evaluar el nivel del servicio prestado.
- Reporte periódico del uso y concepto del usuario sobre el servicio.
- Registro de los requerimientos planteados por el usuario.

Con esta información se puede comenzar a realizar la entrevista para determinar si los servicios proporcionados y planeados por la dirección de Informática cubren las necesidades de información de las dependencias.

A continuación se presenta una guía de cuestionario para aplicarse durante la entrevista con el usuario con su respectivo puntaje para la evaluación posterior.

1. ¿Considera que el Departamento de Sistemas de Información de los resultados esperados?

A. Si ()

B. No ()

2. ¿Cómo considera usted, en general, el servicio proporcionado por el Departamento de Sistemas de Información?

- A) Deficiente ()
- B) Aceptable ()
- C) Satisfactorio ()
- D) Excelente ()

3. ¿Cubre sus necesidades el sistema que utiliza el departamento de cómputo?

- C. No las cubre ()
- D. Parcialmente ()
- E. La mayor parte ()
- F. Todas ()

4. ¿Hay disponibilidad del departamento de cómputo para sus requerimientos?

- A. Generalmente no existe ()
- B. Hay ocasionalmente ()
- C. Regularmente ()
- D. Siempre ()

5. ¿Son entregados con puntualidad los trabajos?

- A) Nunca ()
- B) Rara vez ()
- C) Ocasionalmente ()
- D) Generalmente ()
- E) Siempre ()

6. ¿Que piensa de la presentación de los trabajos solicitados al departamento de cómputo?

A) Deficiente ()

B) Aceptable ()

C) Satisfactorio ()

D) Excelente ()

7. ¿Que piensa de la asesoría que se imparte sobre informática?

A) No se proporciona ()

B) Es insuficiente ()

C) Satisfactoria ()

D) Excelente ()

8. ¿Que piensa de la seguridad en el manejo de la información proporcionada por el sistema que utiliza?

A) Nula ()

B) Riesgosa ()

C) Satisfactoria ()

D) Excelente ()

9. ¿Existen fallas de exactitud en los procesos de información?

A) SI ()

B) NO ()

10. ¿Desearía que se incluyeran nuevos módulos a su Sistema?

A) SI ()

B) NO ()

11. ¿Desearía que se incluyeran nuevos módulos al Sistema?

A) SI ()

B) NO ()

3.1.2 Entrevista al Centro de Computo

PUNTOS DE CONTROL

Los datos son uno de los recursos más valiosos de las organizaciones y, aunque son intangibles, necesitan ser controlados y auditados con el mismo cuidado que los demás inventarios de la organización, por lo cual se debe tener presente:

- a) La responsabilidad de los datos es compartida conjuntamente por alguna función determinada y el departamento de cómputo.
- b) Un problema de dependencia que se debe considerar es el que se origina por la duplicidad de los datos y consiste en poder determinar los propietarios o usuarios posibles (principalmente en el caso de redes y banco de datos) y la responsabilidad de su actualización y consistencia.

- c) Los datos deberán tener una clasificación estándar y un mecanismo de identificación que permita detectar duplicidad y redundancia dentro de una aplicación y de todas las aplicaciones en general.
- d) Se deben relacionar los elementos de los datos con las bases de datos donde están almacenados, así como los reportes y grupos de procesos donde son generados.

Lo primero que se debe evaluar es la entrada de la información y que se tengan las cifras de control necesarias para determinar la veracidad de la información, para lo cual se puede utilizar el siguiente cuestionario:

- 1. Indique el porcentaje de datos que se reciben en el área de captación.
- 2. Indique el contenido de la orden de trabajo que se recibe en el área de captación de datos:

Número de folio () Número(s) de formato(s) ()

Fecha y hora de Recepción, Dpto. ()

Recepción () Usuario ()

Nombre del documento () Nombre responsable ()

Volumen aproximado Clave de cargo

de registro () (Número de cuenta) ()

Número de registros () Fecha y hora de entrega de

Clave del capturista () documentos y registros captados ()

Fecha estimada de entrega ()

3. Indique cuál(es) control(es) interno(s) existe(n) en el área de captación de datos:

Firmas de autorización ()

Recepción de trabajos () Control de trabajos atrasados ()

Revisión del documento () Avance de trabajos ()

fuerza (legibilidad, verificación de datos completos, etc.) ()

Prioridades de captación () Errores por trabajo ()

Producción de trabajo () Corrección de errores ()

Producción de cada operador () Entrega de trabajos ()

Verificación de cifras Costo Mensual por trabajo ()

de control de entrada con las de salida. ()

4. ¿Existe un programa de trabajo de captación de datos?

a) ¿Se elabora ese programa para cada turno?

Diariamente ()

Semanalmente ()

Mensualmente ()

b) La elaboración del programa de trabajos se hace:

Internamente ()

Se les señalan a los usuarios las prioridades ()

c) ¿Que acción(es) se toma(n) si el trabajo programado no se recibe a tiempo?

5. ¿Quién controla las entradas de documentos fuente?

6. ¿En que forma las controla?

7. ¿Que cifras de control se obtienen?

Sistema Cifras que se Observaciones. Obtienen

8. ¿Que documento de entrada se tienen?

Sistemas Documentos Dpto. que periodicidad. Observaciones proporciona el documento

9. ¿Se anota que persona recibe la información y su volumen?

SI NO

10. ¿Se anota a que capturista se entrega la información, el volumen y la hora?

SI NO

11. ¿Se verifica la cantidad de la información recibida para su captura?

SI NO

12. ¿Se revisan las cifras de control antes de enviarlas a captura?

SI NO

13. ¿Para aquellos procesos que no traigan cifras de control se ha establecido criterios a fin de asegurar que la información es completa y valida?

SI NO

14. ¿Existe un procedimiento escrito que indique como tratar la información inválida (sin firma ilegible, no corresponden las cifras de control)?

15. En caso de resguardo de información de entrada en sistemas, ¿Se custodian en un lugar seguro?

16. Si se queda en el departamento de sistemas, ¿Por cuanto tiempo se guarda?

17. ¿Existe un registro de anomalías en la información debido a mala codificación?
18. ¿Existe una relación completa de distribución de listados, en la cual se indiquen personas, secuencia y sistemas a los que pertenecen?
19. ¿Se verifica que las cifras de las validaciones concuerden con los documentos de entrada?
20. ¿Se hace una relación de cuando y a quién fueron distribuidos los listados?
-
21. ¿Se controlan separadamente los documentos confidenciales?
-
22. ¿Se aprovecha adecuadamente el papel de los listados inservibles?
-
23. ¿Existe un registro de los documentos que entran a capturar?
-
24. ¿Se hace un reporte diario, semanal o mensual de captura?
-
25. ¿Se hace un reporte diario, semanal o mensual de anomalías en la información de entrada?
26. ¿Se lleva un control de la producción por persona?
27. ¿Quién revisa este control?
28. ¿Existen instrucciones escritas para capturar cada aplicación o, en su defecto existe una relación de programas?

3.1.3 Control de Operación

La eficiencia y el costo de la operación de un sistema de cómputo se ven fuertemente afectados por la calidad e integridad de la documentación requerida para el proceso en la computadora.

El objetivo del presente ejemplo de cuestionario es señalar los procedimientos e instructivos formales de operación, analizar su estandarización y evaluar el cumplimiento de los mismos.

1. ¿Existen procedimientos formales para la operación del sistema de cómputo?

SI () NO ()

3. ¿Están actualizados los procedimientos?

SI () NO ()

4. Indique la periodicidad de la actualización de los procedimientos:

Semestral ()

Anual ()

Cada vez que haya cambio de equipo ()

5. Indique el contenido de los instructivos de operación para cada aplicación:

Identificación del sistema ()

Identificación del programa ()

Periodicidad y duración de la corrida ()

Especificación de formas especiales ()

Especificación de cintas de impresoras ()

Etiquetas de archivos de salida, nombre, ()

archivo lógico, y fechas de creación y expiración

Instructivo sobre materiales de entrada y salida ()

Altos programados y la acciones requeridas ()

Instructivos específicos a los operadores en caso de falla del equipo ()

Instructivos de reinicio ()

Procedimientos de recuperación para proceso de gran duración o criterios ()

Identificación de todos los dispositivos de la máquina a ser usados ()

Especificaciones de resultados

(cifras de control, registros de salida por archivo, etc.) ()

6. ¿Existen órdenes de proceso para cada corrida en la computadora (incluyendo pruebas, compilaciones y producción)?

SI () NO ()

7. ¿Son suficientemente claras para los operadores estas órdenes?

SI () NO ()

8. ¿Existe una estandarización de las ordenes de proceso?

SI () NO ()

9. ¿Existe un control que asegure la justificación de los procesos en el computador?

(Que los procesos que se están autorizados y tengan una razón de ser procesados.

SI () NO ()

10. ¿Cómo programan los operadores los trabajos dentro del departamento de cómputo?

Primero que entra, primero que sale ()

Se respetan las prioridades, ()

Otra (especifique) ()

11. ¿Los retrasos o incumplimiento con el programa de operación diaria, se revisa y analiza?

SI () NO ()

12. ¿Quién revisa este reporte en su caso?

13. Analice la eficiencia con que se ejecutan los trabajos dentro del departamento de cómputo, tomando en cuenta equipo y operador, a través de inspección visual, y describa sus observaciones.

14. ¿Existen procedimientos escritos para la recuperación del sistema en caso de falla?

15. ¿Cómo se actúa en caso de errores?

16. ¿Existen instrucciones específicas para cada proceso, con las indicaciones pertinentes?

17. ¿Se tienen procedimientos específicos que indiquen al operador que hacer cuando un programa interrumpe su ejecución u otras dificultades en proceso?

18. ¿Puede el operador modificar los datos de entrada?

19. ¿Se prohíbe a analistas y programadores la operación del sistema que programo o analizo?

20. ¿Se prohíbe al operador modificar información de archivos o bibliotecas de programas?

21. ¿El operador realiza funciones de mantenimiento diario en dispositivos que así lo requieran?

22. ¿Las intervenciones de los operadores:

Son muy numerosas? SI () NO ()

Se limitan los mensajes esenciales? SI () NO ()

Otras

(especifique) _____

23. ¿Se tiene un control adecuado sobre los sistemas y programas que están en operación?

SI () NO ()

24. ¿Cómo controlan los trabajos dentro del departamento de cómputo?

25. ¿Se rota al personal de control de información con los operadores procurando un entrenamiento cruzado y evitando la manipulación fraudulenta de datos?

SI () NO ()

26. ¿Cuentan los operadores con una bitácora para mantener registros de cualquier evento y acción tomada por ellos?

Si ()

por máquina ()

escrita manualmente ()

NO ()

27. Verificar que exista un registro de funcionamiento que muestre el tiempo de paros y mantenimiento o instalaciones de software.

28. ¿Existen procedimientos para evitar las corridas de programas no autorizados?

SI () NO ()

29. ¿Existe un plan definido para el cambio de turno de operaciones que evite el descontrol y discontinuidad de la operación.

30. Verificar que sea razonable el plan para coordinar el cambio de turno.

31. ¿Se hacen inspecciones periódicas de muestreo?

SI () NO ()

32. Enuncie los procedimientos mencionados en el inciso anterior:

33. ¿Se permite a los operadores el acceso a los diagramas de flujo, programas fuente, etc. fuera del departamento de cómputo?

SI () NO ()

34. ¿Se controla estrictamente el acceso a la documentación de programas o de aplicaciones rutinarias?

SI () NO ()

¿Cómo? _____

35. Verifique que los privilegios del operador se restrinjan a aquellos que le son asignados a la clasificación de seguridad de operador.

36. ¿Existen procedimientos formales que se deban observar antes de que sean aceptados en operación, sistemas nuevos o modificaciones a los mismos?

SI () NO ()

37. ¿Estos procedimientos incluyen corridas en paralelo de los sistemas modificados con las versiones anteriores?

SI () NO ()

38. ¿Durante cuanto tiempo?

39. ¿Que precauciones se toman durante el periodo de implantación?

40. ¿Quién da la aprobación formal cuando las corridas de prueba de un sistema modificado o nuevo están acordes con los instructivos de operación.

41. ¿Se catalogan los programas liberados para producción rutinaria?

SI () NO ()

42. Mencione que instructivos se proporcionan a las personas que intervienen en la operación rutinaria de un sistema.

43. Indique que tipo de controles tiene sobre los archivos magnéticos de los archivos de datos, que aseguren la utilización de los datos precisos en los procesos correspondientes.

44. ¿Existe un lugar para archivar las bitácoras del sistema del equipo de cómputo?

SI () NO ()

45. Indique como está organizado este archivo de bitácora.

Por fecha ()

- por fecha y hora ()
- por turno de operación ()
- Otros ()

46. ¿Cuál es la utilización sistemática de las bitácoras?

47. ¿Además de las mencionadas anteriormente, que otras funciones o áreas se encuentran en el departamento de cómputo actualmente?

48. Verifique que se lleve un registro de utilización del equipo diario, sistemas en línea y batch, de tal manera que se pueda medir la eficiencia del uso de equipo.

49. ¿Se tiene inventario actualizado de los equipos y terminales con su localización?

SI () NO ()

50. ¿Cómo se controlan los procesos en línea?

51. ¿Se tienen seguros sobre todos los equipos?

SI () NO ()

52. ¿Con que compañía?

Solicitar pólizas de seguros y verificar tipo de seguro y montos.

53. ¿Cómo se controlan las llaves de acceso (Password)?.

3.1.4 Controles de Salida

1. ¿Se tienen copias de los archivos en otros locales?

2. ¿Dónde se encuentran esos locales?

3. ¿Que seguridad física se tiene en esos locales?

4. ¿Que confidencialidad se tiene en esos locales?

5. ¿Quién entrega los documentos de salida?

6. ¿En que forma se entregan?

7. ¿Que documentos?

8. ¿Que controles se tienen?

9. ¿Se tiene un responsable (usuario) de la información de cada sistema? ¿Cómo se atienden solicitudes de información a otros usuarios del mismo sistema?

10. ¿Se destruye la información utilizada, o bien que se hace con ella?

Destruye () Vende () Tira () Otro _____

3.1.5 Orden en el Centro de Computo

Una dirección de Sistemas de Información bien administrada debe tener y observar reglas relativas al orden y cuidado del departamento de cómputo. Los dispositivos del sistema de cómputo, los archivos magnéticos, pueden ser dañados si se manejan en forma inadecuada y eso puede traducirse en pérdidas irreparables de información o en costos muy elevados en la reconstrucción de archivos. Se deben revisar las disposiciones y reglamentos que coadyuven al mantenimiento del orden dentro del departamento de cómputo.

1. Indique la periodicidad con que se hace la limpieza del departamento de cómputo y de la cámara de aire que se encuentra abajo del piso falso si existe y los ductos de aire:

Semanalmente () Quincenalmente ()

Mensualmente () Bimestralmente ()

No hay programa () Otra (especifique) ()

2. Existe un lugar asignado a las cintas y discos magnéticos?

SI () NO ()

3. ¿Se tiene asignado un lugar específico para papelería y utensilios de trabajo?

SI () NO ()

4. ¿Son funcionales los muebles asignados para la cintoteca y discoteca?

SI () NO ()

5. ¿Se tienen disposiciones para que se acomoden en su lugar correspondiente, después de su uso, las cintas, los discos magnéticos, la papelería, etc.?

SI () NO ()

6. Indique la periodicidad con que se limpian las unidades de cinta:

Al cambio de turno () cada semana ()

cada día () otra (especificar) ()

7. ¿Existen prohibiciones para fumar, tomar alimentos y refrescos en el departamento de cómputo?

SI () NO ()

8. ¿Se cuenta con carteles en lugares visibles que recuerdan dicha prohibición?

SI () NO ()

9. ¿Se tiene restringida la operación del sistema de cómputo al personal especializado de la Dirección de Informática?

SI () NO ()

10. Mencione los casos en que personal ajeno al departamento de operación opera el sistema de cómputo:

3.1.6 Evaluación de la configuración en el centro de computo

1. De acuerdo con los tiempos de utilización de cada dispositivo del sistema de cómputo, ¿existe equipo?

¿Con poco uso? SI () NO ()

¿Ocioso? SI () NO ()

¿Con capacidad superior a la necesaria? SI () NO ()

Describe cual es _____

2. ¿El equipo mencionado en el inciso anterior puede reemplazarse por otro mas lento y de menor costo?

SI () NO ()

3. Si la respuesta al inciso anterior es negativa, ¿el equipo puede ser cancelado?

SI () NO ()

4. De ser negativa la respuesta al inciso anterior, explique las causas por las que no puede ser cancelado o cambiado.

5. ¿El sistema de cómputo tiene capacidad de teleproceso?

SI () NO ()

6. ¿Se utiliza la capacidad de teleproceso?

SI () NO ()

7. ¿En caso negativo, exponga los motivos por los cuales no utiliza el teleproceso?

SI () NO ()

8. ¿Cuántas terminales se tienen conectadas al sistema de cómputo?

9. ¿Se ha investigado si ese tiempo de respuesta satisface a los usuarios?

SI () NO ()

11. ¿La capacidad de memoria y de almacenamiento máximo del sistema de cómputo es suficiente para atender el proceso por lotes y el proceso remoto?

SI () NO ()

3.1.7 Seguridad Lógica, Física y Confidencial

3.1.7.1 Seguridad Física

El objetivo es establecer políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de datos, información debido a contingencias como incendio, inundaciones, huelgas, disturbios, sabotaje, etc. y continuar en medio de emergencia hasta que sea restaurado el servicio completo.

Tomando en cuenta lo anterior se elaboro el siguiente cuestionario:

1. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información?

SI () NO ()
2. ¿Existe una persona responsable de la seguridad?

SI () NO ()
3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?

SI () NO ()
4. ¿Existe personal de vigilancia en la institución?

SI () NO ()
5. ¿La vigilancia se contrata?
 - a) Directamente ()
 - b) Por medio de empresas que venden ese servicio ()
6. ¿Existe una clara definición de funciones entre los puestos clave?

SI () NO ()

7. ¿Se investiga a los vigilantes cuando son contratados directamente?

SI () NO ()

8. ¿Se controla el trabajo fuera de horario?

SI () NO ()

9. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?.

SI () NO ()

10. ¿Existe vigilancia en el departamento de cómputo las 24 horas?

SI () NO ()

11. ¿Existe vigilancia a la entrada del departamento de cómputo las 24 horas?

a) Vigilante ? ()

b) Recepcionista? ()

c) Tarjeta de control de acceso ? ()

d) Nadie? ()

12. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?

SI () NO ()

13. Se ha instruido a estas personas sobre que medidas tomar en caso de que alguien pretenda entrar sin autorización?

SI () NO ()

14. El edificio donde se encuentra la computadora esta situado a salvo de:

a) Inundación? ()

b) Terremoto? ()

- c) Fuego? ()
- d) Sabotaje? ()
15. El centro de cómputo tiene salida al exterior al exterior?
- SI () NO ()
16. Describa brevemente la construcción del centro de cómputo, de preferencia proporcionando planos y material con que construido y equipo (muebles, sillas etc.) dentro del centro.
17. ¿Existe control en el acceso a este cuarto?
- a) Por identificación personal? ()
- b) Por tarjeta magnética? ()
- c) por claves verbales? ()
- d) Otras? ()
18. ¿Son controladas las visitas y demostraciones en el centro de cómputo?
- SI () NO ()
19. ¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática?
- SI () NO ()
20. ¿Se vigilan la moral y comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar un posible fraude?
- SI () NO ()
21. ¿Existe alarma para
- a) Detectar fuego(calor o humo) en forma automática? ()
- b) Avisar en forma manual la presencia del fuego? ()

c) Detectar una fuga de agua? ()

d) Detectar magnéticos? ()

e) No existe ()

22. ¿Estas alarmas están

a) En el departamento de cómputo? ()

b) En la cintoteca y discoteca? ()

23. ¿Existe alarma para detectar condiciones anormales del ambiente?

a) En el departamento de cómputo? ()

b) En la cintoteca y discoteca? ()

c) En otros lados ()

24. ¿La alarma es perfectamente audible?

SI () NO ()

25. ¿Esta alarma también está conectada

a) Al puesto de guardias? ()

b) A la estación de Bomberos? ()

c) A ningún otro lado? ()

Otro _____

26. Existen extintores de fuego

a) Manuales? ()

b) Automáticos? ()

c) No existen ()

27. ¿Se ha adiestrado el personal en el manejo de los extintores?

SI () NO ()

28. ¿Los extintores, manuales o automáticos a base de TIPO SI NO

a) Agua, () ()

b) Gas? () ()

c) Otros () ()

29. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?

SI () NO ()

30. ¿Si es que existen extintores automáticos son activador por detectores automáticos de fuego?

SI () NO ()

31. ¿Si los extintores automáticos son a base de agua ¿Se han tomado medidas para evitar que el agua cause mas daño que el fuego?

SI () NO ()

32. ¿Si los extintores automáticos son a base de gas, ¿Se ha tomado medidas para evitar que el gas cause mas daño que el fuego?

SI () NO ()

33. ¿Existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos para que el personal

a) Corte la acción de los extintores por tratarse de falsas alarmas? SI () NO ()

b) Pueda cortar la energía eléctrica SI () NO ()

c) Pueda abandonar el local sin peligro de intoxicación SI () NO ()

d) Es inmediata su acción? SI () NO ()

34. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?

SI () NO ()

35. ¿Sabes que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?

SI () NO ()

36. ¿El personal ajeno a operación sabe que hacer en el caso de una emergencia (incendio)?

SI () NO ()

37. ¿Existe salida de emergencia?

SI () NO ()

38. ¿Esta puerta sólo es posible abrirla:

a) Desde el interior ? ()

b) Desde el exterior ? ()

c) Ambos Lados ()

39. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?

SI () NO ()

40. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?

SI () NO ()

41. ¿Se ha tomado medidas para minimizar la posibilidad de fuego:

- a) Evitando artículos inflamables en el departamento de cómputo? ()
- b) Prohibiendo fumar a los operadores en el interior? ()
- c) Vigilando y manteniendo el sistema eléctrico? ()
- d) No se ha previsto ()

42. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?

SI () NO ()

43. ¿Se limpia con frecuencia el polvo acumulado debajo del piso falso si existe?

SI () NO ()

44. ¿Se controla el acceso y préstamo en la

- a) Discoteca? ()
- b) Cintoteca? ()
- c) Programoteca? ()

45. Explique la forma como se ha clasificado la información vital, esencial, no esencial etc.

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

SI () NO ()

47. Explique la forma en que están protegidas físicamente estas copias (bóveda, cajas de seguridad etc.) que garantice su integridad en caso de incendio, inundación, terremotos, etc.

48. ¿Se tienen establecidos procedimientos de actualización a estas copias?

SI () NO ()

49. Indique el número de copias que se mantienen, de acuerdo con la forma en que se clasifique la información:

0 1 2 3

50. ¿Existe departamento de auditoria interna en la institución?

SI () NO ()

51. ¿Este departamento de auditoria interna conoce todos los aspectos de los sistemas?

SI () NO ()

52. ¿Que tipos de controles ha propuesto?

53. ¿Se cumplen?

SI () NO ()

54. ¿Se auditan los sistemas en operación?

SI () NO ()

55. ¿Con que frecuencia?

a) Cada seis meses ()

b) Cada año ()

c) Otra (especifique) ()

56. ¿Cuándo se efectúan modificaciones a los programas, a iniciativa de quién es?

a) Usuario ()

b) Director de informática ()

c) Jefe de análisis y programación ()

d) Programador ()

e) Otras (especifique)

57. ¿La solicitud de modificaciones a los programas se hacen en forma?

a) Oral? ()

b) Escrita? ()

En caso de ser escrita solicite formatos,

58. Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?

SI () NO ()

59. ¿Existe control estricto en las modificaciones?

SI () NO ()

60. ¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?

SI () NO ()

61. ¿Si se tienen terminales conectadas, ¿se ha establecido procedimientos de operación?

SI () NO ()

62. Se verifica identificación:

a) De la terminal ()

b) Del Usuario ()

c) No se pide identificación ()

63. ¿Se ha establecido que información puede ser acesada y por qué persona?

SI () NO ()

64. ¿Se ha establecido un número máximo de violaciones en sucesión para que la computadora cierre esa terminal y se de aviso al responsable de ella?

SI () NO ()

65. ¿Se registra cada violación a los procedimientos con el fin de llevar estadísticas y frenar las tendencias mayores?

SI () NO ()

66. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones?

¿Cuales son?

()Recepción de documentos _____

()Información Confidencial _____

()Captación de documentos _____

()Cómputo Electrónico _____

()Programas _____

()Discotecas y Cintotecas _____

()Documentos de Salida _____

()Archivos Magnéticos _____

()Operación del equipo de computación _____

()En cuanto al acceso de personal _____

()Identificación del personal _____

()Policia _____

()Seguros contra robo e incendio _____

()Cajas de seguridad _____

()Otras (especifique) _____

3.1.7.2 Seguridad en la utilización del equipo

En la actualidad los programas y los equipos son altamente sofisticados y sólo algunas personas dentro del centro de cómputo conocen al detalle el diseño, lo que puede provocar que puedan producir algún deterioro a los sistemas si no se toman las siguientes medidas:

- 1) Se debe restringir el acceso a los programas y a los archivos.
- 2) Los operadores deben trabajar con poca supervisión y sin la participación de los programadores, y no deben modificar los programas ni los archivos.
- 3) Se debe asegurar en todo momento que los datos y archivos usados sean los adecuados, procurando no usar respaldos inadecuados.
- 4) No debe permitirse la entrada a la red a personas no autorizadas, ni a usar las terminales.
- 5) Se deben realizar periódicamente una verificación física del uso de terminales y de los reportes obtenidos.
- 6) Se deben monitorear periódicamente el uso que se le está dando a las terminales.
- 7) Se deben hacer auditorías periódicas sobre el área de operación y la utilización de las terminales.
- 8) El usuario es el responsable de los datos, por lo que debe asegurarse que los datos recolectados sean procesados completamente. Esto sólo se logrará por medio de los controles adecuados, los cuales deben ser definidos desde el momento del diseño general del sistema.

- 9) Deben existir registros que reflejen la transformación entre las diferentes funciones de un sistema.
- 10) Debe controlarse la distribución de las salidas (reportes, cintas, etc.).
- 11) Se debe guardar copias de los archivos y programas en lugares ajenos al centro de cómputo y en las instalaciones de alta seguridad; por ejemplo: los bancos.
- 12) Se debe tener un estricto control sobre el acceso físico a los archivos.
- 13) En el caso de programas, se debe asignar a cada uno de ellos, una clave que identifique el sistema, subsistema, programa y versión.

También evitará que el programador ponga nombres que nos signifiquen nada y que sean difíciles de identificar, lo que evitará que el programador utilice la computadora para trabajos personales. Otro de los puntos en los que hay que tener seguridad es en el manejo de información. Para controlar este tipo de información se debe:

- 1) Cuidar que no se obtengan fotocopias de información confidencial sin la debida autorización.
- 2) Sólo el personal autorizado debe tener acceso a la información confidencial.
- 3) Controlar los listados tanto de los procesos correctos como aquellos procesos con terminación incorrecta.
- 4) Controlar el número de copias y la destrucción de la información y del papel carbón de los reportes muy confidenciales.

El factor más importante de la eliminación de riesgos en la programación es que todos los programas y archivos estén debidamente documentados.

El siguiente factor en importancia es contar con los respaldos, y duplicados de los sistemas, programas, archivos y documentación necesarios para que pueda funcionar el plan de emergencia.

Equipo, programas y archivos

- Control de aplicaciones por terminal
- Definir una estrategia de seguridad de la red y de respaldos
- Requerimientos físicos.
- Estándar de archivos.
- Auditoría interna en el momento del diseño del sistema, su implantación y puntos de verificación y control.

3.1.7.3 Seguridad al restaurar el equipo

El objetivo del siguiente cuestionario es evaluar los procedimientos de restauración y repetición de procesos en el sistema de cómputo.

1) ¿Existen procedimientos relativos a la restauración y repetición de procesos en el sistema de cómputo?

SI ()

NO ()

2) ¿ Enuncie los procedimientos mencionados en el inciso anterior?

3) ¿Cuentan los operadores con alguna documentación en donde se guarden las instrucciones actualizadas para el manejo de restauraciones?

SI () NO ()

En el momento que se hacen cambios o correcciones a los programas y/o archivos se deben tener las siguientes precauciones:

1) Las correcciones de programas deben ser debidamente autorizadas y probadas.

Con esto se busca evitar que se cambien por nueva versión que antes no ha sido perfectamente probada y actualizada.

2) Los nuevos sistemas deben estar adecuadamente documentados y probados.

3) Los errores corregidos deben estar adecuadamente documentados y las correcciones autorizadas y verificadas.

Los archivos de nuevos registros o correcciones ya existentes deben estar documentados y verificados antes de obtener reportes.

3.1.7.4 Procedimientos de respaldo en el caso de desastre

Los desastres que pueden suceder podemos clasificar así:

a) Completa destrucción del centro de cómputo.

b) Destrucción parcial del centro de cómputo.

- c) Destrucción o mal funcionamiento de los equipos auxiliares del centro de cómputo (electricidad, aire, acondicionado, etc.).
- d) Destrucción parcial o total de los equipos descentralizados.
- e) Pérdida total o parcial de información, manuales o documentación.
- f) Pérdida del personal clave.
- g) Huelga o problemas laborales.

3.1.8 Formularios para el seguimiento y control de la Auditoria de Sistemas

AVANCE DEL CUMPLIMIENTO DEL PROGRAMA DE AUDITORIA EN INFORMÁTICA									
ORGANISMO _____			NUMERO _____			HOJA Nº _____		DE _____	
PERIODO QUE REPORTA _____									
FASE	SITUACION DE LA AUDITORIA			PERIODO REAL DE LA AUDITORIA		DIAS REALES UTILIZADOS	GRADO DE AVANCE	DIAS HOMBRES ESTIMADOS	EXPLICACION DE LAS VARIAC. EN RELACION CON LO PROG.
	Nº INICIADA	EN PROCESO	TERMINADA	INICIADA	TERMINADA				

FORMULARIO PARA EL SEGUIMIENTO DE PROGRAMAS

SISTEMA _____ NÚM. DE _____

SISTEMA _____

FECHA DE INICIO __/__/__

FECHA DE TERMINACIÓN __/__/__

PROGRAMA														CDO. DIF.	FECHA TERMIN.	PERSONA ASIGNADA	
NUM.	NOMBRE	A	B	C	D	E	F	G	H	I	J	K	L				M

SIGNIFICADO DE LAS CLAVES

- | | |
|--|--|
| <ul style="list-style-type: none"> A INTERPRETACIÓN B DIAGRAMACIÓN LÓGICA C CREACIÓN DE PRUEBAS D PRUEBA DE ESCRITORIO E CODIFICACIÓN F CAPTURA G COMPILACIÓN | <ul style="list-style-type: none"> H GENERACIÓN DE PRUEBAS I DEPURACIÓN J PRUEBAS K VERIFICACIÓN DE PRUEBAS L CORRECCIONES M CONCLUIDO |
|--|--|

SEGUIMIENTO DE LAS RECOMENDACIONES DE LA AUDITORÍA EN INFORMÁTICA

PERÍODO QUE SE REPORTA: _____

DIRECCIÓN _____ **HOJA No** _____ **DE** _____

AUDITORÍA A: _____ **FECHA DE TÉRMINO DE LA AUDITORÍA** _____

NUM. OBS.	RECOMENDACIÓN	FECHA ESTIMADA DE RESOL.	FECHA REAL DE RESOL.	MOTIVO POR EL CUAL NO HA SIDO RESUELTA	REPLANTEAMIENTO DE LA SOLUCIÓN	OBSERVACIÓN	FECHA PROBAB. IMPLAN.	RESPONS. DE LA RECOMEN.

FORMATO DE INVENTARIO DE COMPUTADORAS PERSONALES

1. Apellidos Nombres Usuario Principal
2. Fuesto

3. Ubicación y/o Oficina

CPU Marca <input style="width: 100%;" type="text"/> Modelo <input style="width: 100%;" type="text"/> Número de Serie <input style="width: 100%;" type="text"/>	CPU PROCESADOR <input style="width: 100%;" type="text"/> 286, 386, 486, PENT M. Serie <input style="width: 100%;" type="text"/>	MEMORIA <input style="width: 100%;" type="text"/> MB, GB, GGB Variedad <input type="radio"/> SI <input type="radio"/> NO Nro. Bancos <input style="width: 100%;" type="text"/> Slot <input style="width: 100%;" type="text"/>
--	---	--

Disco Duro <input style="width: 100%;" type="text"/> <input style="width: 100%;" type="text"/> MB <input style="width: 100%;" type="text"/> Heads <input style="width: 100%;" type="text"/> Cuind <input style="width: 100%;" type="text"/> Sectores Tecnología IDE <input type="radio"/> SCSI <input type="radio"/> MFM <input type="radio"/> ELL <input type="radio"/> OTRO <input type="radio"/>	Disketera Estado: Activo <input type="radio"/> Inactivo <input type="radio"/> Tipo <input style="width: 100%;" type="text"/> Tarjeta de RED <input type="radio"/> Si <input type="radio"/> No Topología <input style="width: 100%;" type="text"/> Marca <input style="width: 100%;" type="text"/> Mac Adress <input style="width: 100%;" type="text"/> Modelo <input style="width: 100%;" type="text"/>
---	--

Monitor Marca <input style="width: 100%;" type="text"/> Modelo <input style="width: 100%;" type="text"/> Serie <input style="width: 100%;" type="text"/> Color <input style="width: 100%;" type="text"/> Tipo <input style="width: 100%;" type="text"/>	Teclado Marca <input style="width: 100%;" type="text"/> M. Serie <input style="width: 100%;" type="text"/>	Configuración <input style="width: 100%;" type="text"/> Tipo Conector <input style="width: 100%;" type="text"/>
---	---	--

Monitor Marca <input style="width: 100%;" type="text"/>	Modelo <input style="width: 100%;" type="text"/>	M. Serie <input style="width: 100%;" type="text"/>
Tipo de conector MiniDin <input style="width: 100%;" type="text"/>	Din <input style="width: 100%;" type="text"/>	Serial <input style="width: 100%;" type="text"/>

Observaciones
Costo
Capacidad y posibilidad de utilización

Productividad

3.2 ETAPA 2: Identificación de las áreas críticas de riesgos

Esta técnica es un sistema de Puntajes Scoring de evaluación manual de las aplicaciones computarizadas, con el objeto de establecer prioridades para efectos de auditoría sobre la base del análisis de riesgo. Esta evaluación nos servirá para detectar las áreas de mayor interés para la auditoría.

AREAS	FACTORES
- Centro de Computo	- Valor de Activos
- Vicerectorado Administrativo	- Vulnerabilidad al Fraude
- Vicerectorado Académico	- Nivel de modificación al sistema y/o al programa
- Oficina de Servicios Académicos (OSA)	- Software utilizado, en general
- Tesorería	- Recursos de hardware utilizado
- Remuneraciones	- Regularidad y uso de los reportes generados por el sistema
- Economía	
- Abastecimiento y patrimonio	
- Oficina de Investigación	
- Personal	
- Contabilidad	
- Oficina de Admisión	
- Control de Personal	
- Personal	

Tt = Suma total de las ponderaciones

AREAS	CENTRO DE COMPUTO						VICE-ADMINISTRATIVO					
	1	2	3	4	5	Tt	1	2	3	4	5	Tt
1. VALOR DE ACTIVOS			X			3					X	5
2. VULNERABILIDAD AL FRAUDE		X				2				X		4
3. NIVEL DE MODIFICACION AL SISTEMA Y/O AL PROGRAMA	X					1			X			3
4. SOFTWARE UTILIZADO, EN GENERAL					X	5		X				2
5. RECURSOS DE HARDWARE UTILIZADO				X		4		X				2
6. REGULARIDAD Y USO DE LOS REPORTES GENERADOS POR EL SISTEMA		X				2			X			3
TOTAL PUNTAJE	1	4	3	4	5	17	-	4	6	4	5	19

AREAS	VICE-ACADEMICO						O.S.A.					
	1	2	3	4	5	Tt	1	2	3	4	5	Tt
1. VALOR DE ACTIVOS				X		4			X			3
2. VULNERABILIDAD AL FRAUDE				X		4				X		4
3. NIVEL DE MODIFICACION AL SISTEMA Y/O AL PROGRAMA					X	5					X	5
4. SOFTWARE UTILIZADO, EN GENERAL			X			3				X		4
5. RECURSOS DE HARDWARE UTILIZADO			X			3			X			3
6. REGULARIDAD Y USO DE LOS REPORTES GENERADOS POR EL SISTEMA					X	5					X	5
TOTAL PUNTAJE	-	-	6	8	10	24	-	-	6	8	10	24

AREAS	TESORERIA						REMUNERACIONES					
	1	2	3	4	5	Tt	1	2	3	4	5	Tt
FACTS \ PUTJES												
1. VALOR DE ACTIVOS			X			3		X				2
2. VULNERABILIDAD AL FRAUDE			X			3			X			3
3. NIVEL DE MODIFICACION AL SISTEMA Y/O AL PROGRAMA		X				2			X			3
4. SOFTWARE UTILIZADO, EN GENERAL			X			3				X		4
5. RECURSOS DE HARDWARE UTILIZADO			X			3		X				2
6. REGULARIDAD Y USO DE LOS REPORTES GENERADOS POR EL SISTEMA			X			3			X			3
TOTAL PUNTAJE	-	2	15	-	-	17	-	4	9	4	-	17

AREAS	ECONOMIA						ABASTEC.Y PATRIMONIO					
	1	2	3	4	5	Tt	1	2	3	4	5	Tt
FACTS \ PUNTS												
1. VALOR DE ACTIVOS			X			3	X					1
2. VULNERABILIDAD AL FRAUDE			X			3			X			3
3. NIVEL DE MODIFICACION AL SISTEMA Y/O AL PROGRAMA		X				2		X				2
4. SOFTWARE UTILIZADO, EN GENERAL		X				2		X				2
5. RECURSOS DE HARDWARE UTILIZADO		X				2		X				2
6. REGULARIDAD Y USO DE LOS REPORTES GENERADOS POR EL SISTEMA			X			3			X			3
TOTAL PUNTAJE	-	6	9	-	-	15	1	6	6	-	-	13

AREAS	OFICINA DE INVESTIGACION						PERSONAL					
	1	2	3	4	5	Tt	1	2	3	4	5	Tt
1. VALOR DE ACTIVOS		X				2		X				2
2. VULNERABILIDAD AL FRAUDE	X		X			3						1
3. NIVEL DE MODIFICACION AL SISTEMA Y/O AL PROGRAMA	X		X			3						1
4. SOFTWARE UTILIZADO, EN GENERAL	X		X			3						1
5. RECURSOS DE HARDWARE UTILIZADO	X	X				2						1
6. REGULARIDAD Y USO DE LOS REPORTES GENERADOS POR EL SISTEMA	X		X			3						1
TOTAL PUNTAJE	5	4	12	-	-	16	-	-	-	-	-	7

AREAS	CONTABILIDAD						OF.ADMISION					
	1	2	3	4	5	Tt	1	2	3	4	5	Tt
1. VALOR DE ACTIVOS	X					1			X			3
2. VULNERABILIDAD AL FRAUDE	X					1		X		X		4
3. NIVEL DE MODIFICACION AL SISTEMA Y/O AL PROGRAMA		X				2			X			3
4. SOFTWARE UTILIZADO, EN GENERAL	X					1				X		4
5. RECURSOS DE HARDWARE UTILIZADO	X					1			X			3
6. REGULARIDAD Y USO DE LOS REPORTES GENERADOS POR EL SISTEMA		X				2		X		X		4
TOTAL PUNTAJE	4	4	-	-	-	8	-	4	9	12	-	21

FACTS \ PTES	AREAS		CONTROL DE PERSONAL				
	1	2	3	4	5	Total	
1. VALOR DE ACTIVOS		X				2	
2. VULNERABILIDAD AL FRAUDE			X			3	
3. NIVEL DE MODIFICACION AL SISTEMA Y/O AL PROGRAMA		X				2	
4. SOFTWARE UTILIZADO, EN GENERAL			X			3	
5. RECURSOS DE HARDWARE UTILIZADO		X				2	
6. REGULARIDAD Y USO DE LOS REPORTES GENERADOS POR EL SISTEMA			X			3	
TOTAL PUNTAJE	-	6	9	-	-	15	

FACTS \ PTAJES	AREAS		PERSONAL				
	1	2	3	4	5	Total	
1. VALOR DE ACTIVOS		X				2	
2. VULNERABILIDAD AL FRAUDE			X			3	
3. NIVEL DE MODIFICACION AL SISTEMA Y/O AL PROGRAMA			X			3	
4. SOFTWARE UTILIZADO, EN GENERAL			X			3	
5. RECURSOS DE HARDWARE UTILIZADO		X				2	
6. REGULARIDAD Y USO DE LOS REPORTES GENERADOS POR EL SISTEMA			X			3	
TOTAL PUNTAJE	-	4	12	-	-	16	

**RESULTADO DEL PUNTAJE SCORING PARA DETERMINAR
LAS AREAS CRITICAS**

AREAS	PUNTAJE
Oficina de Servicios Académicos	24
Vice rectorado Académico	24
Contabilidad	21
Vice rectorado Administrativo	19
Centro de Cómputo	17
Tesorería	17
Remuneraciones	17
Personal	16
Control de Personal	15
Economía	15
Abastecimiento y Patrimonio	13
Oficina de Admisión	8
Oficina de Investigación	7

- En este cuadro los resultados también resumen las prioridades de cada área, por consiguiente la de mayor puntaje requieren mas atención por parte de la organización.

TABLA DE EVALUACION APLICABLE AL
ANALISIS DE RIEGOS

CALIFICACION	INTERVALO
EXCELENTE	26 – 30
BUENO	21 – 25
REGULAR	15 – 20
DEFICIENTE	7 – 14
PESIMO	0 – 6

3.3 ETAPA 3: Calculo del impacto y evaluación de riesgos

LA EVALUACION RESULTA DE RESPONDER LOS CUESTIONARIOS DE PREGUNTAS ANTERIORES APLICADAS A LA UNIVERSIDAD UANCV.

3.3.1 Calculo del análisis del riesgo de la eficiencia en el servicio

RESULTADO DE LA EVALUACIÓN POR AREAS CON REFERENCIAS EN LA ENTREVISTA A USUARIOS

Nº	PREGS AREAS	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	Total	Puntaj
1	O.S.A	B	B	A	D	D	B	B	E	B	B	A	3.9	11
		0	0.5	0	1	0.75	0.3	0.3	0	1	0	0		
2	VICE-ACADEMIC	A	C	C	D	D	B	B	E	B	B	A	5.82	16
		1	0.75	0.6	1	0.75	0.3	0.3	0	1	0	0		
3	CONTABILIDAD	B	A	B	B	B	B	B	A	B	B	A	2.74	7
		0	0.25	0.3	0.25	0.25	0.3	0.3	0	1	0	0		
4	VICE-ADMINIST	A	B	B	D	D	B	B	B	B	B	A	4.57	12
		0	0.5	0.3	1	0.75	0.3	0.3	0.3	1	0	0		
5	TESORERIA	B	B	A	B	B	C	A	B	A	B	A	1.9	5
		0	0.5	0	0.25	0.25	0.6	0	0.3	0	0	0		
6	REMUNERACION	B	A	B	C	C	C	A	B	B	B	A	3.82	11
		0	0.25	0.3	0.75	0.5	0.6	0	0.3	1	0	0		
7	PERSONAL	B	B	B	C	C	C	A	E	B	B	A	3.74	10
		0	0.5	0.3	0.75	0.5	0.6	0	0	1	0	0		
8	CONTROL DE PERSONAL	A	A	B	B	C	C	A	B	B	B	A	4.32	12
		1	0.25	0.3	0.25	0.5	0.6	0	0.3	1	0	0		
9	ABASTEC. Y PATRIMONIO	A	B	C	C	C	C	A	E	A	B	A	4.01	11
		1	0.5	0.6	0.75	0.5	0.6	0	0	0	0	0		
10	ECONOMIA	A	B	B	C	C	C	A	E	B	B	A	4.74	13
		1	0.5	0.3	0.75	0.5	0.6	0	0	1	0	0		
11	OF.DE ADMISIÓN	B	B	B	B	C	C	A	E	A	B	A	2.24	6
		0	0.5	0.3	0.25	0.5	0.6	0	0	0	0	0		
12	OF.DE INVESTIG.	A	B	B	B	C	C	A	E	A	B	A	2.24	6
		0	0.5	0.3	0.25	0.5	0.6	0	0	0	0	0		

Promedio Eficiencia = 10.00 (DEFICIENTE)

3.3.2 Resultado del análisis del riesgo de seguridad lógica y física

Auditoría	Tópico	Puntaje	Calificación
Desarrollo de Sistemas	Análisis	4	Pésimo
	Diseño Lógico	2	Pésimo
	Desarrollo de Sistemas	1	Pésimo
	Control de Proyectos	1	Pésimo
	Control de Diseños de Sistemas y Programación	2	Pésimo
	Instructivos de Operación	0	Pésimo
	Formas de Implementación	0	Pésimo
Punto de control	Datos	13	Deficiente
	Operación	10	Deficiente
	Salida	14	Deficiente
	Almacenamiento	7	Deficiente
	Mantenimiento	13	Deficiente
Rendimiento	Orden en el Centro de Cómputo	24	Bueno
	Configuración del Sistema	6	Pésimo
Seguridad	Lógica y Confidencial	6	Pésimo
	Física	21	Bueno
	Utilización del Equipo	17	Regular
	Restauración del Equipo	10	Deficiente
	Casos de Desastres	9	Deficiente

PROMEDIO SEGURIDAD= 8.42 (DEFICIENTE)

(*) Conclusiones a los cuestionarios anteriores sobre seguridad lógica y física.

3.3.3 Resultado del análisis del riesgo de eficacia en el servicio

(Cuestionario incluido)

CONTROLES	RPTA	PUNTAJE
Existen planes a largo plazo para el departamento de informática.	SI	10
Valore la conexión de esos planes con los planes generales de la empresa.		10
Cubren los planes del D.I. los objetivos a largo plazo de la empresa, valórelo.	NO	5
Existe un comité de planificación o dirección del departamento de informática.	NO	5
Dicho comité está compuesto por directivos de departamentos de usuario.	NO	2
Valore la congruencia entre los planes a largo y corto plazo del D.I.		20
Son adecuados los recursos asignados al D.I. para cumplir con los objetivos a corto plazo.	NO	7
Existe una adecuada vía de comunicación y control de cumplimiento de objetivos a corto y largo plazo por parte de la dirección.	NO	10
Valore la precisión en el cumplimiento de los planes a corto plazo del D.I.		6
Existen políticas para la planificación, control y evaluación del D.I.	NO	4
Evalúe la integración de las directivas de política de alta dirección en el D.I.		18
Existen estándares que regulen la explotación de recursos del D.I.	SI	10
Evalúe la calidad y vigencia de los estándares de explotación de recursos del D.I.		10
Evalúe el cumplimiento de los estándares de explotación de recursos del D.I.		10
Existen procedimientos sobre las responsabilidades, peticiones de servicio y relaciones entre los diferentes departamentos y el D.I.	SI	7
Dichos procedimientos están adecuadamente distribuidos en los diferentes departamentos.		7
Evalúe el cumplimiento de dichos procedimientos por parte de los diferentes departamentos.		7
El D.I. está separado orgánicamente en la estructura orgánica de la empresa.	SI	5
Es independiente la ubicación del D.I. de los otros departamentos de la empresa.	SI	5
Están claramente definidas las unidades organizativas en el D.I.	SI	7
Están separadas las unidades de desarrollo de sistemas y explotación.	SI	3
Están separadas las unidades de explotación y control de datos.	SI	4
Están separadas las unidades de administración de bases de datos y desarrollo de sistemas.	SI	4

Evalúe la independencia de las funciones del personal entre las diferentes unidades.		2
¿Existe una descripción por escrito (manual de operaciones y procedimientos) de cada puesto de trabajo en las diferentes unidades de D.I.?	NO	5
¿La descripción del puesto de trabajo incluye definiciones de conocimientos y pericia técnicos?	NO	2
¿Los manuales de operaciones y procedimientos pasan una revisión mínima anual?	NO	2
¿Existe un método de evaluación para cubrir las vacantes del D.I.?	NO	3
Evalúe la adecuación del método y políticas de selección para cubrir las antedichas vacantes.		2
Evalúe la conformidad del personal del D.I. con las políticas y el sistema de promoción.		25
¿Existe un programa de orientación, formación y reciclaje de personal de planilla?	SI	10
¿Tiene una revisión al menos anual dicho programa de reciclaje?	SI	10
¿Supone el programa de reciclaje al menos el 10% del presupuesto del D.I.?	NO	2
Valore la formación interna recibida en el programa de reciclaje.		7
¿Cuál es la valoración que da el personal al programa de formación y reciclaje?		9
Contraste y evalúe la adecuación entre las fichas de formación del personal y las exigencias de conocimientos o pericia necesaria de los puestos.		7
¿Existe algún método de control y evaluación de consecución de objetivos de cada puesto de trabajo?	SI	14
¿Está informado y comprende el personal el sistema de evaluación sobre consecución de objetivos?	SI	15
¿Existe algún sistema de control para la carga de trabajo del D.I.?	SI	20
¿Ha establecido el D.I. prioridades de tratamiento de los diferentes trabajos?	SI	17
Evalúe el exceso de capacidad de los equipos disponibles para satisfacer la demanda en la época baja de proceso		20
Evalúe la capacidad de los recursos humanos para satisfacer la demanda en la época alta de proceso .		26
Evalúe el exceso de capacidad de los recursos humanos disponibles para satisfacer la demanda en la época baja de proceso .		24
¿Qué valoración le dan los trabajadores del área de explotación a la disponibilidad de recursos humanos en épocas altas de trabajo ?		20

¿Existe un calendario de mantenimiento preventivo de material o lógico?	SI	15
¿Realiza la dirección del D.I. un control y seguimiento del flujo de trabajo y de las variaciones del calendario de explotación?	NO	7
¿Se registran las variaciones del calendario de explotación?	NO	3
¿Existe un registro de problemas de tratamiento de datos?	SI	10
¿Se toman acciones directas para evitar la recurrencia de los problemas de tratamiento de datos?	SI	10
¿Existe un procedimiento de selección de logical acorde con los planes a corto y largo plazo de la empresa?	NO	4
¿Se lleva a cabo dicho procedimiento a la hora de analizar necesidades de logical?		2
Evalúe la satisfacción de los usuarios de software respecto a la última adquisición.	SI	12
¿Existe algún procedimiento de prueba antes de efectuar cambios de logical de sistemas?	SI	15
¿Existe alguna persona especializada en implementación de logical de sistemas?	SI	10
¿Existe algún registro sobre los cambios realizados sobre el logical del sistema?	SI	7
¿Se corresponde la implantación del sistema de informática distribuida o red con las especificaciones de los planes a corto y largo plazo de la empresa?	SI	17
¿Se han desarrollado planes de implantación conversión y pruebas de aceptación para la red de informática distribuida de la empresa?	NO	4
¿Ha sido desarrollado dicho plan conjuntamente por el departamento de informática y la dirección de los departamentos usuarios afectados?	SI	4
¿Contempla dicho plan de aceptación de estándares de implantación, conversión y pruebas en redes informáticas distribuidas?	SI	12
¿Ha sido desarrollado el logical del sistema de acuerdo con la metodología del ciclo de desarrollo de sistemas de la organización o mediante una metodología cimentada y reconocida?		10
¿Incluye el plan de implantación o conversión de la red de informática distribuida?	SI	12
¿Se ha contemplado en el plan cualquier riesgo especial asociado a las redes distribuidas?	NO	3
¿Existen procedimientos de control generales de la red de informática distribuida?	NO	4
¿Se realizarán dichos procedimientos de control con una periodicidad mínima mensual?	SI	11
¿Son analizados los cambios de los procedimientos operativos para ver si responden a necesidades reales de los usuarios?	SI	15

¿Ha establecido el departamento de informática controles sobre utilización de los contenidos de las bases de datos de la red?	SI	20
¿Aseguran dichos controles la estandarización de las definiciones de datos compartidos?	SI	24
¿Se mantienen diccionarios de datos comunes a los diferentes usuarios de las bases de datos?	SI	7
¿Existe un sistema eficaz para evitar que los usuarios cambien la definición de datos comunes de las bases?	SI	17
¿Existe una comunicación regular sobre cambios efectuados en las bases de datos comunes?	NO	5
¿Existe algún control que asegure que los cambios introducidos en los contenidos de la base de datos mantienen la compatibilidad de dichas bases?	NO	2
¿Existe algún procedimiento establecido que asegure en todos los puntos de la red que los cambios críticos en los contenidos de las bases se lleven a cabo con puntualidad?	NO	3
¿Se ha establecido una política para identificación y clasificación de datos sensibles de la red?	NO	2
¿Existen mecanismos de seguridad que impidan introducciones o modificaciones erróneas de datos sensibles?	SI	16
¿Existe algún mecanismo de control que asegure una adecuada carga de la red especialmente en los períodos de trabajo crítico?	SI	10
¿Se han establecido y comunicado a los usuarios procedimientos efectivos para coordinar la operación de los programas de aplicación y la utilización de los contenidos de las B.D.?	NO	1
¿Poseen todos los usuarios de la red especificaciones sobre disponibilidad, horarios, tiempo de respuesta, almacenamiento, respaldo y control operativo?	NO	2
¿Se realizan reuniones periódicas entre los usuarios para coordinar calendarios de explotación, especificaciones de tratamiento y procedimientos operativos?	NO	1
¿Establecen todas las instalaciones de departamentos usuarios de la red previsiones sobre necesidades de material fungible?		4
¿Existe siempre un remanente de material fungible que asegure la continuación de los procesos en los departamentos usuarios?		5
¿Existen procedimientos establecidos por el departamento de informática para la gestión y control del logical de comunicaciones?		6
¿Están incluidas en dicho procedimiento estándares sobre la utilización de dicho logical?		6

¿Se han remitido descripciones escritas sobre los citados procedimientos a todos los departamentos usuarios?	NO	3
¿Se han establecido prioridades de transmisión asignadas a los mensajes enviados por la red?	NO	1
Evalúe la satisfacción de los usuarios sobre las transmisiones a través de la red, sobre todo en períodos críticos.		6
¿Existen planes de formación para usuarios de la red?	NO	2
¿Existen responsables que evalúen el correcto uso de la red por parte de los usuarios?	SI	22
¿Están perfectamente identificados todos los elementos físicos de la red (unidades de control, módem cables, etc.) mediante etiquetas externas adecuadas?	SI	25
¿Está asegurando en un tiempo prudencial la reparación o cambio de elementos físicos de la red?	SI	17
¿Se realiza por parte de personal especializado una revisión periódica de todos los elementos de la red?	SI	30
¿Existe algún sistema para controlar y medir el funcionamiento del sistema de informática distribuida de la red?	SI	27
¿Existe una estructura que asegure que la explotación de máxima prioridad se lleva a cabo y se transmite en primer lugar?	NO	4
¿Se han desarrollado o adquirido procedimientos automáticos para resolver o evitar cierres del sistema (abrazos mortales)?	SI	16
¿Existe una rutina que asegure que ningún proceso o dato de baja prioridad va a estar sin procesar indefinidamente en la red?	SI	20
¿Existen mecanismos que controlen los tiempos de respuesta de la red y la duración de los fallos de operación de la misma?	SI	20
¿Se controlan regularmente todos los procesadores de la red?	SI	18

PROMEDIO EFICACIA = 9.843 (DEFICIENTE)

3.4 ETAPA 4: Creación del Informe Final

3.4.1 Información relativa a la Auditoría de Sistemas

3.4.1.1 Motivo del Examen

La Auditoría de Sistemas realizada a la Gestión Académica y Administrativa de la Universidad Andina Nestor Cáceres Velasquez de Juliaca se ha efectuado en cumplimiento a la recomendación de la Carrera Académico Profesional de Ingeniería de Sistemas, en razón de los indicios de la existencia de problemas que no permiten una eficiente utilización de los recursos informáticos.

3.4.1.2 Naturaleza y Objetivos

La presente acción de control tiene la naturaleza de Auditoría de Sistemas, con los siguientes objetivos:

1. Objetivo General

Verificar la operatividad, funcionalidad y gestión de los sistemas de información y computación.

2. Objetivos Específicos

Evaluar y diagnosticar:

- Fraude y errores de los sistemas de aplicación e información.
- Verificar la conformidad y eficacia de los sistemas.
- Organización del servicio.

- Mantenimiento de los sistemas.
- Métodos, normas y documentación de los sistemas.
- Métodos de explotación de los sistemas de computación (computadores).
- Seguridad física.
- Confidencialidad.

3.4.1.3 Alcance

La acción de control se ha realizado de acuerdo con las Normas de Auditoría Generalmente Aceptadas y habiendo comprendido la revisión y análisis de los sistemas de información y computación a cargo de la Oficina de Informática de la UANCV abarcando el período de Agosto a Diciembre de 1999.

El desarrollo de la presente Auditoría se ha visto limitado considerablemente, por las siguientes razones:

La desorganización de la Oficina de Informática.

1. La carencia de documentación sobre los sistemas de información, normas y/o procedimientos.
2. La inexistencia de funciones definidas.
3. La carencia de una estructura funcional formal de la Oficina de Informática.
4. La Inexperiencia del personal de la Oficina de Informática.
5. El desorden en el inventario de los equipos de computación.
6. El desconocimiento de los usuarios sobre el alcance de los sistemas de información de su competencia.

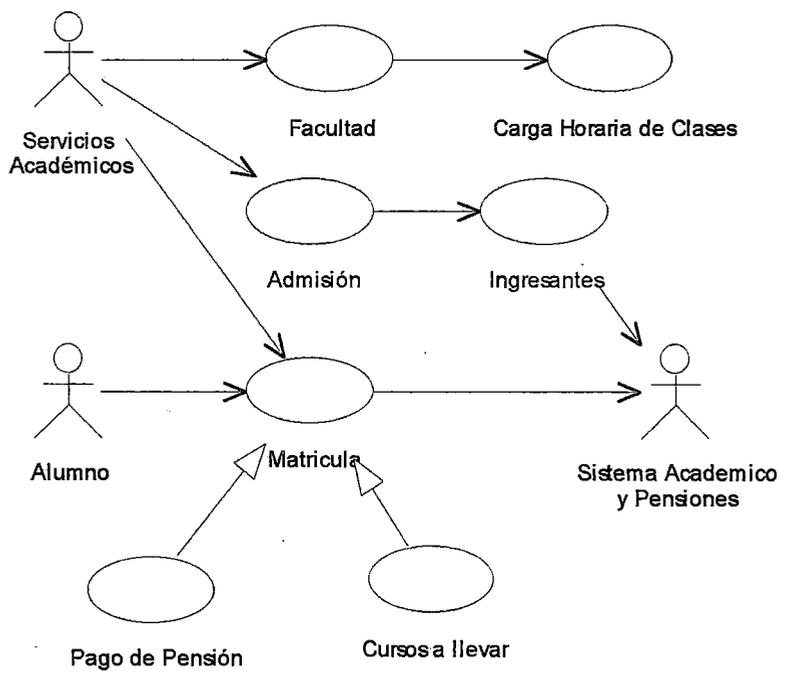
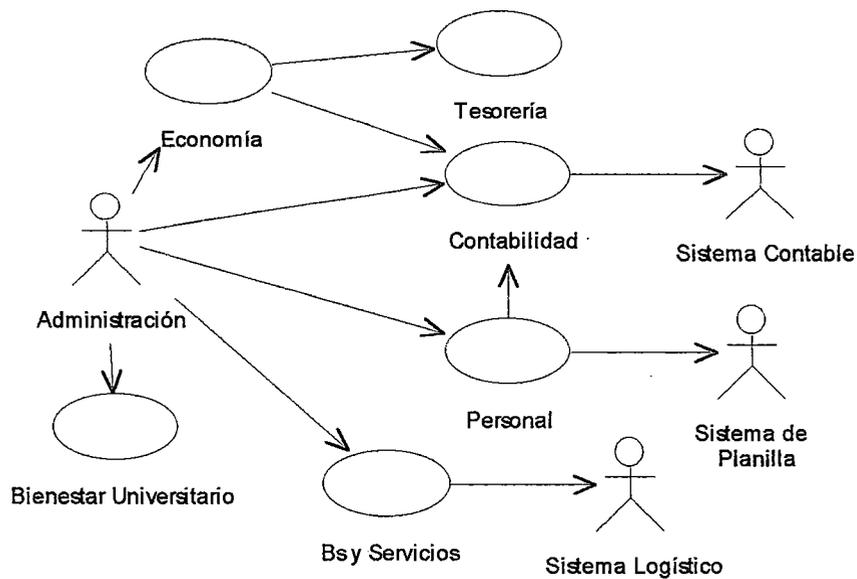
3.4.1.4 Situación actual de las oficinas en la UANCV incluido el centro de

cómputo

Es necesario tener conocimiento de la situación actual en cuanto a equipamiento de cada facultad, oficinas y además dependientes, con el propósito de establecer las condiciones adecuadas de hardware y software a fin de poner en práctica un sistema de comunicación que permita altas velocidades de transmisión local y remota, fiabilidad, seguridad en la transmisión y soporte para la creación de nuevas tecnologías como lo es la construcción de un sitio web e Intranet.

Cabe recalcar que la información referente a la situación actual de las oficinas administrativas y los sistemas de conjunto de todas las dependencias de la Universidad fue obtenida aplicando método de entrevista a cada responsable de área. La información obtenida como es de suponer depende en gran medida de la colaboración de los responsables de área en cada dependencia.

3.4.1.5 Diagrama del funcionamiento actual del sistema de información de la UANCV



Rectorado

La Sede principal del rectorado se encuentra ubicado en el Edificio el Campin Pasaje la Cultura s/n, Cercado Juliaca. Está constituido por 4 oficinas o departamentos, estos son:

- 1.- Secretaría General.
- 2.- Oficina de Planificación Universitaria.
- 3.- Oficina de Comunicaciones y Relaciones Públicas.
- 4.- Oficina de Asesoría legal.

La Secretaría general, se encuentra ubicado en el 3er Piso del mencionado Edificio, cuenta con 2 computadoras Pentium y una impresora instalada en un pequeño ambiente. Dispone de 2 líneas telefónicas, una de ellas es directa permitiendo el acceso a Internet.

La Oficina de Planificación Universitaria, se encuentra ubicado en el 4to piso, cuenta con 4 computadoras Pentium y compatibles 486, 2 impresoras matriciales, a pesar de contar con una conexión física de red, sus computadoras no están conectadas a esta, no cuenta con línea propia.

La oficina de imagen institucional y relaciones públicas se encuentra ubicado en el 3er piso, cuenta con 2 computadoras, Pentium y compatible 486, cuenta con una línea

propia, su labor se basa en difundir la imagen de la Universidad, se encuentra con conexión de red en forma física, pero no está conectada a sus computadoras.

La oficina de Asesoría legal, se encuentra en el 3er piso, cuenta con 2 computadoras, compatibles 486, y una impresora matricial, no cuenta con línea telefónica. No existe personal técnico permanente para dar soporte a estos equipos, empleando en su lugar servicios técnicos externos temporalmente. Cada área reserva su información debido a la importancia que representa para la Universidad. La instalación de una red en este lugar dependería en gran medida de la correcta administración (seguridad) por parte de personal especializado.

La información que se procesa en el rectorado es información netamente confidencial por lo que es catalogado como información de emisión crítica.

Vice-Rectorado Académico

El Vice-Rectorado Académico está constituido por:

- La Oficina permanente de Admisión.
- La Oficina de Servicios Académicos.
- La Oficina de Investigación.
- La Oficina de Extensión Universitaria y Proyección Social.

La Oficina Permanente de Admisión, se encuentra ubicado en el 2do piso, cuenta con una computadora Pentium, y una impresora matricial, no se encuentra conectada a una red, no cuenta con una línea telefónica propia.

La Oficina de Servicios Académicos se encuentra entre en el 2do y 3er Piso, cuenta con 9 computadoras Pentium y compatible 486 y 5 impresoras matriciales, en esta oficina una de sus dependencias es el centro de cómputo, la biblioteca Central de la Unidad Educativa e Implementación. Unidad de registro central, Unidad de Archivo Central.

El Centro de Cómputo actualmente se desempeña como el principal centro de procesamiento de datos de la Universidad. Su principal función se enfoca en el proceso académico, destacando los procesos de matrícula, gestión de notas e identificación de docentes, etc. A pesar de contar con una conexión de una red ethernet, par trenzado y topología estrella, las computadoras no se encuentran conectadas. El Sistema Operativo para estos equipos es Windows 95 y DOS Pentium de 120 y 333 Mhz. 8,16 y 24 Mb de RAM, 1.6 Mb de H.D. Se tiene planeado a corto plazo conectarse a la red local a fin de integrar el centro de cómputo con el área administrativa, para ello disponen con la mayoría de equipos de red, no disponen de personal calificado, tanto para el desarrollo de aplicaciones como para el mantenimiento de los sistemas existentes, no cuentan con conexiones Wan.

La Oficina de Investigación, se encuentra en el 3er Piso, cuenta con 1 computadora compatible 486 y una impresora matricial, no cuenta con una línea telefónica. La oficina de Extensión Universitaria y Proyección Social, se encuentra ubicado en la sede de la ciudad de Puno, contando con CAPS de derecho, Obstetricia, Ingeniería Civil, Ingeniería de Sistemas y Contabilidad con 25 computadoras Pentium y Compatibles 486, con 2 impresoras matriciales y con una línea propia, no se encuentran conectados a una red, mucho menos cuentan con una conexión física, el Sistema Operativo con que operan las máquinas es Windows 95, todos los gestiona administrativas son operadas en la ciudad de Juliaca.

Vice-Rectorado Administrativo

El Vice-Rectorado Administrativo (VRAD) esta constituido por :

- Oficinas de Producción y Prestación de Servicios.
- Oficinas de Bienestar Universitario.
- Oficina de Economía.
- Oficina de Personal.

La Oficina de Producción y prestación de servicios se encuentra ubicado en el 3er piso, cuenta con una computadora Pentium y una compatible 486 y una impresora matricial, no cuenta con una línea telefónica.

La Oficina de Bienestar Universitario, esta conformado por la oficina de Asistencia social, Unidad de salud, Unidad de recreación deportiva y la Unidad de servicios, cuenta con una computadora compatible 486 y una impresora matricial.

La oficina de economía, esta oficina está conformada por la unidad de contabilidad, caja, unidad de tesorería y la unidad de abastecimiento patrimonial y mantenimiento, cuenta con 14 computadoras Pentium y compatibles 486 con 10 impresoras matriciales, cuenta con 2 líneas telefónicas propias, están conectados a Internet temporalmente a excepción de las demás dependencias esta oficina si se encuentra conectada a una red ethernet, con cableado par trenzado UTP, con topología estrella, cuenta con un Hub de 14 terminales, por los que utilizan 10 máquinas, el Sistema Operativo con que todos se ejecutan bajo Novell 4.1 de 32 bits, versión en castellano, el servidor con que cuentan es una Pentium II –Intel Celeron, 333 Mhz, de 64 Mb de RAM vienen operando todas las dependencias de esta oficina a excepción de la unidad de caja.

La oficina de personal, cuenta con 2 computadoras Pentium y una compatible 386, dos impresoras matriciales, también forma parte de la red antes mencionada no cuentan con soporte técnico, los servicios de mantenimiento externo.

FACULTADES

FACULTAD DE CIENCIAS DE LA EDUCACION

Ubicación : Centro Comercial N° Dos Tercer piso

Laboratorio de Cómputo: No cuentan con ningún laboratorio de cómputo

Area Administrativa :

- 2 Computadoras compatibles 486, 1 Pentium
- 2 Impresoras Matriciales
- Sistemas Operativos Windows 95 y DOS

Observaciones:

- No dispone de red local para el área administrativa y académica
- No cuenta con personal técnico permanente.
- No tienen proyectado al corto plazo interconectar todas las dependencias, así como disponer de una conexión al Internet por circuitos digitales.
- Cuenta con acceso al Internet por medio de la red telefónica básica.

FACULTAD DE CIENCIAS JURIDICAS Y POLITICAS – DERECHO

Ubicación : Centro Comercial N° Dos, tercer Piso.

Laboratorio de Cómputo:

- No cuenta con ningún laboratorio de cómputo.

Area Administrativa :

- 04 Computadoras Pentium de 300 y 333 Mhz
- Sistema Operativo Windows 95

Observaciones :

- No dispone de una red local para el área administrativa y académica.
- No cuenta con personal técnico permanente.
- Disponen de acceso al Internet por la red telefónica básica.

FACULTAD DE CIENCIAS DE LA SALUD

CARRERA ACADEMICA PROFESIONAL DE OBSTETRICIA

Ubicación : Centro Comercial N° Tres, tercer piso.

Laboratorio de Cómputo

- No cuenta con ningún laboratorio de cómputo.

Area Administrativa :

- 02 Computadoras Pentium de 133 y 300 Mhz

Observaciones :

- No disponen de red local para el área administrativa y académica.
- No disponen de acceso al Internet a pesar de contar con una línea propia.

CARRERA ACADEMICO PROFESIONAL DE ENFERMERIA

Ubicación : Centro Comercial N° Tres, tercer Piso

Laboratorios de Cómputo

- No cuentan con ningún laboratorio de cómputo.

Area Administrativa

- 01 Computadoras Pentium 133 Mhz

Observaciones :

- No disponen de red local para el área académica y administrativa.
- No cuentan con personal técnico permanente.
- Cuentan con acceso al Internet por medio de la red telefónica básica

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y CONTABLES

**CARRERA ACADEMICO PROFESIONAL DE ADMINISTRACION Y
MARKETING**

Ubicación : Centro Comercial N° Tres, Segundo Piso

Laboratorios de Cómputo : 01

- 12 Computadoras Pentium de 233 Mhz

Area Administrativa

- 01 Computadora Pentium II de 300 Mhz

Observaciones :

- No disponen de red local para el área académica y administrativa
- No cuentan con personal técnico permanente.
- No se encuentran conectadas por una red.

CARRERA ACADEMICO PROFESIONAL DE CONTABILIDAD

Ubicación: Centro Comercial N° 3, Segundo Piso

Laboratorio de Cómputo:

- No cuenta con ningún laboratorio de cómputo.

Area Administrativa:

- 01 Computadora Pentium de 133 Mhz

Observaciones:

- No disponen de red local para el área administrativa y académica.
- No disponen de acceso al Internet a pesar de contar con una línea propia.

FACULTAD DE INGENIERIA Y CIENCIAS PURAS

CARRERA ACADEMICO PROFESIONAL DE INGENIERIA CIVIL

Ubicación : Ciudad Universitaria, 3er Piso, Taparachi

Laboratorio de Cómputo:

- No cuenta con ningún laboratorio de cómputo.

Area Administrativa:

- 01 Computadoras compatible 486 de 100 Mhz

Observaciones:

- No existe ningún tipo de comunicación local.
- No cuenta con soporte técnico permanente
- No cuenta con una línea telefónica propia.

CARRERA ACADEMICO PROFESIONAL DE INGENIERIA DE SISTEMAS

Ubicación : Ciudad Universitaria, 2do Piso, Taparachi

Laboratorio de Cómputo: 01

- 10 Computadoras Pentium II 333 Mhz
- 7 Computadoras Pentium I 133 Mhz

Laboratorio de Ensamblaje: 01

- 06 Computadoras 486 compatible

Area Administrativa :

- 01 Computadora Pentium compatible 200 Mhz

Observaciones :

- Cuenta con red Novell 3.11 y Windows NT
- Cuenta con línea telefónica con Internet

CARRERA ACADEMICO PROFESIONAL DE MECANICA

Ubicación : Ciudad Universitaria, 1er Piso, Taparachi

Laboratorio de Cómputo :

- No cuenta con ningún laboratorio de cómputo.

Area Administrativa:

- 02 computadoras compatibles 486DX 80 Mhz.

Observaciones:

- No disponen de red local para el área académica y administrativa.
- No cuenta con una conexión a Internet por no tener una línea telefónica propia.

INSTITUTO DE INFORMATICA

Ubicación : Centro Comercial N° 3 – 2do Piso

Laboratorios de Cómputo : 01

- 07 Computadoras compatibles Pentium I - 133 Mhz .
- 09 Pentium II de 250 Mhz

Sala de Servidor

- 01 Servidor Pentium II de 333 Mhz, servidor principal, servicios activos de Web Server, Correo Electrónico, FTP y Base de Datos, Sistemas Operativos UNIX Solaris ó Windows NT-Server.

Area Administrativa:

- 01 Computadora Pentium de 133 Mhz

Observaciones :

- El laboratorio, se encuentra en proceso de implementación, con una red LAN topología estrella.
- Por medio del servicio de acceso remoto instalado en un servidor Windows NT o UNIX Solaris, es posible dar acceso a usuarios remotos al Internet, para disponer de una línea telefónica exclusiva a este servicio.
- La Administración de equipos se encuentra bajo la supervisión permanente de técnicos especializados.
- Su Objetivo inmediato es constituirse como centro proveedor de información con acceso al Internet, perfilándose con ello como nodo central para dar salida a Internet desde diferentes puntos remotos.

PROGRAMA DE EXTENSION UNIVERSITARIA DE PUNO

Ubicación : Ciudad de Puno

Laboratorio de Cómputo : 01

- 20 Computadoras compatibles y Pentium de 100 Mhz

Area Administrativa

- 02 Computadoras compatibles 486DX de 100 Mhz

Observaciones

- No disponen de red local para el área académica y administrativa.
- No cuentan con personal técnico permanente.
- Tienen planeado a mediano plazo adquirir nuevos equipos de cómputo.
- El laboratorio no se encuentra conectado en red.

3.4.2 Conclusiones

- En la oficina de Servicios Académicos y el área de Contabilidad se tiene un servicio deficiente por no dar los resultados esperados, no existe un control proactivo sino existe un control reactivo de la información. No existe la garantía de la integridad de información que parte del sistema debido a la cadencia de sistema de controles detectivos y corruptivos, en el caso del vicerrectorado no hay mucha relevancia porque el manejo es más documentario, pero cabe resaltar que también falta un subsistema de trámites documentarios. En cuanto a las demás

áreas de servicio es deficiente y en el caso de tesorería es pésima por no estar integrado al sistema.

- El mayor riesgo económico está concentrado en las áreas de los Vicerrectorados Académico y Administrativo, la oficina de servicios académicos (OSA) y la oficina de Contabilidad (ver tabla del puntaje scoring).
- La Eficiencia en el servicio debido al cambio de las estructuras por la que ha pasado el Área de Informática, no se evidencia en las áreas a los responsables de llevar un seguimiento de la evolución de los principales sistemas y los corporativos, tampoco se evidencia la presencia de los auditores de sistemas de la Inspectoría General en el desarrollo del sistema para evaluar que la información requerida por el usuario quede cubierta y se cumpla con el grado de control que necesita la información procesada por el sistema, de acuerdo con los objetivos y políticas de la Institución.
- La Eficacia del servicio es deficiente en promedio, si bien es cierto que se garantiza de alguna manera la continuidad del sistema no se puede afirmar lo mismo del desarrollo del sistema y sus tiempos de respuesta.
- La Seguridad Lógica Se ha evidenciado que los sistemas verificados no están registrados en INDECOPI.
- No todas las Facultades y Áreas cuentan con los UPS y estabilizadores en los servidores de red, para evitar la pérdida de información en los principales sistemas corporativos (SGH y ICC), ante cualquier eventualidad.

3.4.3 Observaciones

1. No existe políticas de control.
2. La Planificación de centros de cómputo no tiene coherencia con el plan estratégico de la Universidad.
3. El desarrollo de sistemas es incipiente.
4. No se cumplen con las normas de control y soporte de los recursos de información.
5. No se evidencia responsabilidad sobre el acceso, seguridad, mantenimiento y control de hardware.
6. El software existente no cuenta con procedimientos de acceso, seguridad, mantenimiento y control.
7. Organización inadecuada.
8. Falta de personal estable.
9. Contratación irregular de personal.
10. Carencia de estándares y documentación.
11. Falta de políticas y planes de sistemas.
12. Demanda insatisfecha de sistemas de computación y de información de las áreas.
13. Falta de atención a los usuarios por parte de la Oficina de Informática.
14. Contrato Licencia de Uso de software oneroso y sin seguridades jurídicas ni técnicas.
15. Adquisiciones de hardware sin estudio de requerimientos.
16. Desarrollo de software sin estudio de respaldo.

17. Inexistencia de normas y procedimientos para copias de seguridad.
18. Sistema de Contabilidad incompleto, ineficiente e inseguro.
19. Sistema de Personal inadecuado, ineficiente e inseguro.
20. Sistema de Transporte, inseguro.
21. Acceso indebido a la información.
22. Administración inadecuada de los recursos de computación.
23. No existe registro del funcionamiento y ocurrencia de los sistemas.
24. No existen normas ni procedimientos para pruebas de implantación.
25. No existen programas de mantenimiento de los sistemas de computación.
Faltante de periféricos.
26. Instalaciones eléctricas y de datos defectuosos.
27. Seguridad física inadecuada.
28. No se cuenta con licencias de software.
29. Bases de datos con información inconsistente.

3.4.4 Recomendaciones

1. Que el rector disponga que la oficina de racionalización, ubique al centro de cómputo dependiendo de la dirección universitaria (rectorado). Asimismo se efectúe una revisión de sus funciones como área de apoyo de servicio informático a todas las unidades organizacionales de la Universidad debiendo considerar las siguientes funciones principales:
 - a. Planeamiento de los sistemas de información.

- b. Análisis y Diseño de los Sistemas de Información, Construcción e Implantación de los sistemas de información.
 - c. Mantenimiento de los sistemas de información y computación.
 - d. Mantener la operatividad de los Sistemas de Información y computación.
2. Considerando que la falta de una dirección calificada ha sido el permanente cuello de botella en el desarrollo del Centro de Cómputo desde que esta entró en funcionamiento es conveniente que la misma esta a cargo de un profesional que acredite experiencia y calificación, que su contratación se realice a través de una empresa externa especializada en selección de personal, lo que estaría garantizando la seriedad e idoneidad del proceso de evaluación y selección. Dicha acción deberá cumplirla la Dirección de personal en coordinación con la Dirección Universitaria (rectorado). Considerando que esta última debe depender en adelante del centro de cómputo.
3. El jefe de centro de cómputo con el apoyo de la oficina de racionalización, debe elaborar los estándares, normas y procedimientos para desarrollar adecuadamente las tareas y funciones del área. Así mismo elaborarán y actualizarán la documentación de los sistemas de información.
4. La Oficina general de presupuesto y planificación debe proveer el plan estratégico de la Institución del centro de cómputo, para que a partir de éste, dicha oficina sustente su plan estratégico de desarrollo de sistemas de Información, a través de un proyecto integral, en coordinación con las áreas usuarias de los comités de usuarios que deberán crearse para este fin específico.

5. La OVRA debe disponer la cancelación del sistema (S.I.I) ya que al tenerse un contrato vigente con la empresa (M&S), siendo el sistema (SIM). Un proyecto de similares características no está debidamente sustentado la necesidad de su ejecución.
6. El centro de cómputo deberá efectuar un estudio de demanda de sistemas de información y cómputo de las diferentes áreas de la UANCV, para el soporte de sus actividades y la posterior centralización de la información para la toma de decisiones. Este estudio será la base para elaborar el plan estratégico de sistemas, además permitirá priorizar el desarrollo de los sistemas de información.
7. Como se indicó en nuestro informe preliminar, de no cumplir la empresa (M&S SYSTEMS) con los plazos establecidos para el desarrollo de los sistemas bajo licencia de uso, se recomienda mejorar dicho contrato. En caso de no ser viable la resolución de este, centro de cómputo recepcionará los sistemas, materia del contrato, sometidos, necesariamente, a planes de prueba donde participan los usuarios de los sistemas y den la conformidad del caso.
8. El centro de cómputo debe tomar la potestad de los sistemas de contabilidad, personal y académica, por razones de funcionalidad, seguridad y control también deberá retirar los programas fuentes, restringir el acceso a las bases de datos, etc. Y asumir el mantenimiento (Atención de los requerimientos del usuario), mejorar su diseño para eliminar el ingreso duplicado de la información así como velar por su seguridad de sus datos, en el más breve plazo. Además documentará los sistemas para que los usuarios puedan operarlos correctamente, así como para

- B. La Auditoría de sistemas mejoró la ejecución de los exámenes de la auditoría de sistemas en la UANCV, permitiendo detectar anomalías y sugerir medidas correctivas.
- C. La Auditoría de Sistemas, propone un modelo estándar de premisas que describen situaciones de riesgo que se dan en cualquier organización.
- D. Se recomienda a la Dirección de la Universidad motivarse mas en estos aspectos tecnológicos y poner mas énfasis en el centro de informática si se quiere crear una Universidad altamente eficaz y seria.
- E. Se recomienda al centro de cómputo presentar un plan de auditoria mensual sobre los reportes elaborados.

Se recomienda al centro de cómputo elaborar un plan de auditoría semestral, sobre la integridad de la información.

3.6 Bibliografía

1. Seguridad en Computación William P. Martín, Interface Age, febrero 1984.
2. Information System Management. Jame A. Senn, State University of New York Bringhamtor, Wadsworth Publishing Company, Inc. Belmont California 1978.
3. Management Information and Control System, R. I Trickner Oxford Center for Management Studies, Willer – Interscience Publication 1976.
4. La computación en México Diagnóstico, Perspectiva y Estrategias de Desarrollo, Fundación Arturo Rosembleuth, A.C, 1982.
5. Metodología y Técnicas de Investigación en Ciencia Sociales, Felipe Pardiñas, Siglo XXI, 1981.
6. Revistas de Comunidad Informática, Secretaria de Programación y Presupuesto.
7. Information Systems in Management, Reston Publishing Company, Inc. Prentice Hall Company, La Edition, Reston, Virginia.
8. Auditoria de Sistema Electrónico. Porter, Jr. W. Thomas. Herrero Hermanos, Sucs. S.A., 2 a. edición, México, D.F.
9. Auditoria de Sistemas en Funcionamiento. José Dagoberto Pinilla Febrero 1997.
10. ISACA : “CISA REVIEW MANUAL” - Edition 2000
11. ISACA : “COBIT : Control Objectives for Information and related technologies” – Edition 2000.

5. Seguridad en Computación William P. Martín, Interface Age, febrero 1984.
6. Information System Management. Jame A. Senn, State University of New York Bringhamtor, Wadsworth Publishing Company, Inc. Belmont California 1978.
7. Management Information and Control System, R. I Trickner Oxford Center for Management Studies, Willer – Interscience Publication 1976.
8. La computación en México Diagnóstico, Perspectiva y Estrategias de Desarrollo, Fundación Arturo Rosembleuth, A.C, 1982.
9. Metodología y Técnicas de Investigación en Ciencia Sociales, Felipe Pardinás, Siglo XXI, 1981.
10. Revistas de Comunidad Informática, Secretaria de Programación y Presupuesto.
11. Information Systems in Management, Reston Publishing Company, Inc. Prentice Hall Company, La Edition, Reston, Virginia.
12. Auditoria de Sistema Electrónico. Porter, Jr. W. Thomas. Herrero Hermanos, Sucs. S.A., 2 a. edición, México, D.F.
13. Auditoria de Sistemas en Funcionamiento. José Dagoberto Pinilla Febrero 1997.
14. ISACA : “CISA REVIEW MANUAL” - Edition 2000
15. ISACA : “COBIT : Control Objectives for Information and related technologies” – Edition 2000.

3.7 Glosario de Términos

Autor

Persona natural que realiza la creación intelectual.

Actos Ilegales

Los actos ilegales se refieren a infracciones a las leyes o reglamentos gubernamentales cometidas por las entidades. Los actos ilegales son atribuibles a la entidad, cuyos estados financieros son objetos de auditoría, o actos cometidos por la gerencia o los empleados que la representen. Tales actos pueden involucrar la manipulación, la falsificación o la modificación de los registros o documentos, la malversación de activos, la eliminación u omisión de los efectos de las transacciones en los registros o documentos, el registro de transacciones sin sustento o la aplicación errónea de normas contables.

Auditor Gubernamental

Personas que forman parte del Sistema Nacional de Control y tiene la responsabilidad final de la auditoría. El término “auditor” ; se usa también para referirse al personal de las sociedades de auditoría independiente, que es designado para examinar los estados financieros de entidades del estado.

Auditoría de Gestión

Es un examen objetivo, sistemático y profesional de evidencias, realizado con el fin de proporcionar una evaluación independiente sobre el desempeño (rendimiento) de una entidad, programa o actividad gubernamental, orientado a mejorar la efectividad, eficiencia y economía en el uso de los recursos públicos, así como el control gerencial para facilitar la toma de decisiones por quienes son responsables de adoptar acciones correctivas y, mejorar la responsabilidad ante el público.

Acceso limitado

Es un tipo de acceso que permite acceder, a los diferentes usuarios, únicamente a niveles autorizados y parciales a algún servicio y/o información.

Backbone

espina dorsal

En comunicaciones, parte de una red que soporta el mayor tráfico. Puede interconectar múltiples localidades, y pueden conectarse redes más pequeñas a ésta.

Backup

seguridad, respaldo]

Recursos adicionales o copias de datos en diferentes medios de almacenamiento como prevención contra emergencias.

Batch

Lote, grupo

Grupo o colección de ítems. Programa por lote o trabajo por lote, se refiere a un programa que procesa un conjunto entero de datos, por ejemplo, un programa de informes o de clasificación.

Browser

Es un programa amigable y fácil de usar que se utiliza para acceder a los servicios de Internet. Antes de que existieran los browsers, se necesitaba saber una serie de complicados comandos para ver los recursos en el Internet. Los browsers más conocidos son Netscape y Explorer.

Base de Datos

Compilación de obras, hechos o datos en forma impresa, en unidad de almacenamiento de ordenador o de cualquier otra forma

Contraloría General de la República

Es el Órgano rector del Sistema Nacional de Control, tiene autonomía técnica, funcional, administrativa y financiera. Determina las funciones de los órganos del sistema y su propia estructura organizativa.

Control Interno

Es un proceso continuo realizado por la dirección y gerencia y, otros empleados de la entidad, para proporcionar seguridad razonable, respecto a si están lográndose los objetivos siguientes:

- Promover la efectividad, eficiencia y economía en las operaciones y, la calidad en los servicios que debe brindar cada entidad pública;
- Proteger y conservar los recursos públicos contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal
- Cumplir las leyes, reglamentos y otras normas gubernamentales; y,
- Elaborar información financiera válida y confiable presentada con oportunidad

Competencia profesional

Es la cualidad que caracteriza al Auditor por el nivel de Idoneidad y habilidad profesional que ostenta para efectuar su labor acorde con las exigencias que demanda la auditoría. La competencia profesional puede apreciarse en el conocimiento de las entidades gubernamentales y los métodos y procedimientos necesarios para la auditoría gubernamental, así como en el entrenamiento y experiencia que requiere la aplicación de tales conocimientos en el trabajo.

Cuidado profesional

Significa emplear correctamente el criterio para determinar el alcance de la auditoría y para seleccionar los métodos, procedimientos y técnicas de auditoría que deben

aplicarse. Ello pone de manifiesto la responsabilidad del auditor en cuanto a cumplir con las normas de auditoría gubernamental.

Confidencialidad

Conlleva a mantener estricta reserva respecto al proceso y los resultados de la Auditoría, no revelando los hechos, datos y situaciones que sean de conocimiento del auditor por el ejercicio de su actividad profesional. Solo podrá acceder a la información relacionada con el examen, el personal vinculado directamente con la dirección y ejecución del trabajo de auditoría.

Control de Calidad

El Conjunto de Políticas y procedimientos, así como recursos técnicos especializados para cerciorarse que las auditorías se realizan de acuerdo con los objetivos, políticas, normas y procedimientos de Auditoría gubernamental.

Código de Ética

Constituye un grupo de reglas heterónomas, es decir son obligatorias en función del vínculo jurídico que las une, sin embargo, este conjunto de normas sólo son guías mínimas de orientación, puesto que el deber concreto en situaciones particulares que afronta cada auditor gubernamental, reside en los principios generales de los propios códigos y en los principios generales de los propios códigos y en los principios de la ética inscritos al interior del hombre.

Correo Electrónico o Mail

En general es un sistema de comunicaciones que permite enviar y recibir mensajes como archivos entre diferentes usuarios previamente identificados con una dirección electrónica de correo, brindando también Internet este servicio.

Certeza de Auditoría

El nivel de satisfacción que el auditor posee con respecto a la confiabilidad de una aseveración efectuada por una parte, para el uso de otras partes. La satisfacción del auditor se deriva de dos fuentes:

- La efectividad del control interno para prevenir o detectar errores e irregularidades significativas en las aseveraciones de los estados financieros.
- La evidencia persuasiva de auditoría (obtenida de los procedimientos de auditorías) con respecto a si las aseveraciones de los estados financieros carecen de errores e irregularidades significativos.

Data cartridge

cartucho de datos

Módulo de cinta magnética removible.

Evidencia de auditoría

Viene a ser la información que obtiene el auditor para extraer conclusiones en las cuales basar su opinión. La evidencia de auditoría abarca los documentos fuentes y los registros contables que sustentan los estados financieros y la información corroborativa provenientes de otras fuentes.

Etica

Está constituida por valores morales que permiten a la persona adoptar decisiones y determinar un comportamiento apropiado, esos valores deben estar basado en lo que es correcto, lo cual puede ir más allá de lo que es legal.

Examen Especial

Comprende la revisión y análisis de una parte de las operaciones o transacciones, efectuadas con posterioridad a su ejecución, con el objeto de verificar el cumplimiento de los dispositivos legales y reglamentarios aplicables y elaborar el correspondiente informe que incluya conclusiones, observaciones y recomendaciones. El Examen Especial puede incluir una combinación de objetivos financieros y operativos o, restringirse a sólo uno de ellos, dentro de un área limitada o asunto específicos de las operaciones.

Entrenamiento Técnico

Está constituido por la preparación en la metodología, procedimiento y técnicas de auditoría y la actualización continua, así como el desarrollo de habilidades y destrezas necesarias para asegurar la calidad del trabajo de auditoría.

Efectividad

La efectividad tiene relación directa con el logro de los objetivos y metas programados. Eficiencia. Se refiere a la relación existente entre los bienes y servicios producidos (productividad) y su comparación con un estándar de desempeño establecido.

Economía

Se relaciona con la adquisición de bienes y/o servicios en condiciones de calidad, cantidad apropiada y oportuna entrega, al mínimo costo posible.

Gateway

puerta de acceso

Computador que interconecta y realiza la conversión de protocolos entre dos tipos de redes. Por ejemplo, una puerta de acceso entre una red LAN de computadoras personales y una red de *mainframe*.

Host

anfitrión

Computador central en un entorno de procesamiento distribuido. Por lo general, se refiere a un gran computador de tiempo compartido o un computador central que controla una red.

Hub

eje, centro

Dispositivo de comunicación central para líneas de comunicaciones en una topología de estrella. Es posible que no agregue nada a la transmisión (eje pasivo) o puede contener dispositivos electrónicos que regeneren las señales para incrementar la fuerza, así como la actividad del monitor (eje pasivo, eje inteligente).

Hallazgos de Auditoría

Son asuntos que llaman la atención del auditor y que en su opinión, deben comunicarse a la entidad, ya que representan deficiencias importantes que podrán afectar en forma negativa, su capacidad para registrar, procesar, resumir y reportar información financiera, de acuerdo con las aseveraciones efectuadas por la gerencia en los estados financieros. Pueden referirse a diversos aspectos de la estructura de Control Interno, tales como: ambiente de control, sistema de contabilidad y procedimientos de control.

Internet

Es una red constituida por computadoras conectadas entre si mediante líneas de comunicación especial a nivel mundial, que permite intercambiar, buscar, consultar, almacenar y comunicarse con diferentes usuarios de todo el mundo, para obtener la más variada información (en forma de Imagen, sonido, textos o programas entre otras), para fines comerciales, intercambio de conocimientos, comunicaciones, negocios, etc.

Independencia

Es la cualidad que permite apreciar que los juicios formulados por el auditor estén fundados en elementos objetivos de los aspectos examinados. La objetividad es la actitud de independencia mental que debe de mantener el auditor en la ejecución de la auditoría, es decir, no deben permitir que el prejuicio, las ideas preconcebidas o la influencia de terceros se impongan sobre su imparcialidad. La integridad implica que el auditor debe ser recto y honesto al realizar su trabajo.

Información confidencial

Es toda información que, previa evaluación, ha sido clasificada como del más alto valor para la institución, y que su conocimiento así como su divulgación por personas no autorizadas, generaría graves daños a la Institución.

Importancia relativa

Magnitud o naturaleza de un monto erróneo, incluyendo una omisión en la información financiera que, ya sea individualmente o en total, a la luz de las circunstancias, hace probable que se vea influido el juicio de una persona razonable que confía en la información, o que su decisión sea afectada como resultado de tales errores u omisiones.

Incertidumbre

Asuntos cuyos resultados o consecuencias dependen de acciones o hechos futuros que no están bajo el control directo de la entidad pero que pueden afectar a los estados financieros.

Mecanismo de Encriptación

Es una técnica que permite guardar una información de manera confidencial.

Moral

Es el conjunto de valores o principios que se asume como modelos ideales de comportamiento. Se fortalece la moral en una entidad, cuando el personal ha sido adecuadamente seleccionado y ubicado.

Normas Técnicas

Son procedimientos normativos específicos para un área determinada

Objetividad

Implica que la auditoría debe efectuarse sobre la base de una evaluación objetividad de los hechos rodeada de imparcialidad y libre de influencias que pudieran deteriorar las conclusiones derivadas de las evidencias obtenidas.

Programa de Ordenador (Software)

Expresión de un conjunto de instrucciones mediante palabras, códigos, planes o en cualquier otra forma que, al ser incorporadas en un dispositivo de lectura automatizada, es capaz de hacer que un computador ejecute una tarea u obtenga un resultado. La protección del programa de ordenador comprende también la documentación técnica y los manuales de uso.

Plan de Contingencias

Es un documento de carácter confidencial que describe los procedimientos que debe seguir la Oficina e Informática para actuar en caso de una emergencia que interrumpa la operatividad del sistema de computo.

Papeles de Trabajo

Registra el planeamiento, naturaleza, oportunidad y alcance de los procedimientos de auditoría aplicados por el auditor; y los resultados conclusiones extraídas de la evidencia obtenida. Se utilizan para controlar el progreso del trabajo y proveer evidencia del trabajo realizado para respaldar la opinión del auditor. Los papeles de

trabajo pueden estar constituidos por datos conservados en papel, película, medio electrónicos u otros medios.

Programa de Auditoría

Establece la naturaleza, oportunidad y alcance los procedimientos de auditoría planeados y que se requieren para implementar el plan de auditoría. El programa de auditoría sirve como conjunto de instrucciones para los asistentes que participan en el examen y como un medio de control de la debida ejecución del trabajo.

Pruebas de controles

La aplicación de procedimientos de auditoría para obtener evidencia de auditoría sobre la efectividad del diseño y la operación de aquellas actividades dentro de la estructura del proceso de control interno que constituyen de un enfoque basado en sistemas con respecto a uno o mas de los objetivos de auditoría. Las pruebas de controles normalmente incluyen cierta combinación de indagación observación y/o inspección de documentos y pueden incluir otras técnicas de auditoría que incluyan cálculos y comparación.

Pruebas de detalles

Las pruebas de detalle son la aplicación de uno o mas de las técnicas de auditoría a las partidas o transacciones individuales que constituyen el saldo de una cuenta o clase de transacciones.

Procedimiento de Auditoría

Comprende la aplicación de una técnica de auditoría para obtener evidencia. Los procedimientos de Auditoría pueden agruparse en tres conjuntos que son:

- Pruebas de controles
- Procedimientos analíticos
- Pruebas de detalles

Plan de Sistemas de Información

Es una herramienta de gestión que establece las necesidades de información de la entidad. Tiene el propósito de prever el desarrollo de los recursos físicos y lógicos con un horizonte temporal determinado, de manera que contribuya efectivamente con los objetivos de la entidad.

Procedimientos Analíticos

La aplicación de comparaciones, cálculos, indagaciones, inspecciones y observaciones para analizar y desarrollar las expectativas con respecto a relaciones entre los datos financieros y de operación para compararlos con los saldos de cuentas o clase de transacciones que se hayan registrado. Los procedimientos analíticos incluyen pruebas de razonabilidad, análisis de tendencias y análisis de relación.

Prueba de doble propósito

Una prueba que se desempeña para obtener evidencia de auditoría que satisfaga los objetivos de las pruebas de controles y las pruebas de detalles al mismo tiempo.

Programas sensitivos

Es un programa de aplicación cuyas modificaciones no autorizadas con propósitos fraudulentos puede resultar en pérdida o apropiación ilícita de activos físicos o financieros de la Institución.

Riesgo de auditoría

El riesgo de que el auditor emita inadvertidamente una opinión de auditoría sin salvedad sobre estados financieros que contengan errores e irregularidades de importancia relativa.

Riesgo de control

El riesgo de que los controles internos no prevengan o detecten y corrijan oportunamente los errores e irregularidades significativos que puedan ocurrir.

Riesgo inherente

La posibilidad de que ocurran errores o irregularidades significativos, sin considerar el efecto del control interno.

Riesgo de detención

El riesgo de que nuestros procedimientos, sustantivos de auditoría no detecten errores e irregularidades significativas.

Riesgo Muestral

Riesgo que surge de la posibilidad de que las conclusiones del auditor, basadas en muestras, puedan ser diferentes de las conclusiones a que habría llegado si la población muestral completa hubiera sido sometida al mismo procedimiento de auditoría.

RAID (Redybdabt Arrays of Inexpensive Disks)

arreglos redundantes de discos no costosos

Agrupamiento de discos en el cual los datos se copian en múltiples unidades. Proporciona un caudal de procesamiento más rápido, tolerancia de fallas (espejos) y corrección de errores.

Responsabilidad

Es el deber de los funcionarios o empleados de rendir cuenta ante una autoridad superior y ante el público por los fondos o bienes del Estado a su cargo y/o por una misión u objetivo encargado y aceptado.

Constituye un concepto que tiene una relación directa con la moral del individuo que guía su propia conciencia y se refleja en las creencias y compromisos sociales,

culturales, religiosos, fraternales, cívicos e ideológicos, adquiridos durante su existencia.

Riesgo Tecnológico

Revisar el riesgo tecnológico se realizara a través de la medición del riesgo de cada área para posteriormente calcular en promedio el riesgo total, por lo que los puntos importantes para la medición se encuentran reflejados en el “Procedimientos para Determinar el Nivel de Riesgo Tecnológico”.

También para medir el riesgo tecnológico se puede aplicar el FODA (Fuerza, Oportunidades, Debilidades y Amenazas), siendo rescatable señalar las fortalezas (actividades desarrolladas por las entidades tendientes a disminuir el riesgo causado por las deficiencias existentes) y deficiencias o debilidades identificadas en las diferentes áreas examinadas. Determinan un aporte mas para calcular el riesgo tecnológico total. Por lo que se deberá tomar en cuenta lo siguiente:

- Indicadores funcionales de riesgo.
- Relacionados con datos sensibles.
- Involucrados con los Ingresos y Egresos.
- Relacionado con las transferencias de activos.
- Indicadores técnicos de riesgo.
- El sistema es complejo.
- Tiene muchas interfaces o interfaces complejas.

- No se encuentra bien documentada.
- Se tiene una tecnología compleja.
- Se tiene problemas con el desempeño.
- Se desarrollo los sistemas usando un lenguaje nuevo o complejo.

También es necesario indicar que existe un riesgo de auditoría en el proceso de la acción de control, como de la evaluación del riesgo tecnológico y esta se refiere al hecho que al examinar parte de la información disponible en vez de toda, inadvertidamente el auditor emita un informe que exprese una opinión de auditoría sin salvedades sobre lo observado afectados por una distorsión.

Seguridad

Es el conjunto de medidas técnicas educacionales, médicas y psicológicas empleadas para prevenir accidentes, eliminar las condiciones inseguras del ambiente, e instruir o convencer a las personas, acerca de la necesidad de implantación de practicas preventivas.

Sistema de Información

Esta constituido por los métodos y procedimientos establecidos para registrar, procesar, resumir e informar sobre las operaciones de una entidad. La calidad de la información que brinda el sistema afecta la capacidad de la gerencia para adoptar decisiones adecuadas que permitan controlar las actividades de la entidad.

Sistema Nacional de Control

Tiene por objetivo la evaluación periódica de los resultados de la gestión pública, dentro de criterios de economía, eficiencia, eficacia y transparencia; y del ejercicio de las funciones de los servidores y funcionarios públicos; en relación al cumplimiento de la normatividad y de los objetivos y metas propuestas, a fin de formular recomendaciones que permitan contribuir al desarrollo de la Administración Gubernamental

Sistema

Cualquier conjunto cohesionado de elementos que están dinámicamente relacionados para lograr un propósito determinado.

Satélite

Todo dispositivo situado en el espacio extraterrestre, apto para recibir y transmitir o retransmitir señales.

SQL (Structured Query Language)

lenguaje de consulta estructurado

Lenguaje utilizado para interrogar y procesar datos en una base de datos relacional.

Desarrollado originalmente por IBM para su *mainframe*, ha habido muchas implementaciones creadas para aplicaciones de base de datos en mini y microcomputadores. Los comandos SQL pueden utilizarse para trabajar

interactivamente con una base de datos, o pueden incluirse en un lenguaje de programación para servir de interfaz a una base de datos.

Técnicas de auditoría

Los mecanismos mediante los cuales los auditores recopilan la evidencia de auditoría.

Las técnicas de auditoría consisten en: comparación, cálculo, confirmación, indagación, inspección, observación, y examen físico.

TCP/IP (Transmission Control Protocol/Internet Protocol)

protocolo de control de transmisiones/protocolo Internet

Protocolos de comunicaciones desarrollados bajo contrato del Departamento de Defensa de los Estados Unidos para intercomunicar sistemas diferentes..

LAN (Local Área Network)

red de área local

Red de comunicaciones que sirve a usuarios dentro de un área geográficamente limitada. La LAN está compuesta por servidores de archivos, que contiene los programas y las bases de datos, y por computadores personales o estaciones de trabajo (clientes), que realizan el procesamiento de la aplicación.

Licencia

Es la autorización o permiso que concede el titular de los derechos (licénciate) al usuario de la obra u otra producción protegida (licenciatarío), para utilizarla en una

forma determinada y de conformidad con las condiciones convenidas en el contrato de licencia. A diferencia de la cesión la licencia no transfiere la titularidad de los derechos.

UPS (Uninterruptible Power Supply)

fuerza de alimentación ininterrumpible

Energía de seguridad par aun sistema de computación cuando lá energía eléctrica se interrumpe o baja a un nivel de voltaje inaceptable.

Usuario

Toda persona que hace uso de un recurso informático.

VIRUS

Software usado para destruir datos en un computador. Después que se escribe el código del virus, se oculta en un programa existente. Una vez que el programa se ejecuta, el código del virus también se activa y agrega copias de sí mismo a otros programa en el sistema. Los programas infectados copian el virus a otros programas.

VMS

(Virtual Memory System)

sistema de memoria virtual

Sistema operativo utilizado en series VAX de Digital. Las aplicaciones VMS se ejecutan en cualquier VAX, desde el MicroVAX hasta el VAX más grande.

(Voice Messaging System)

sistema de mensajería vocal

Véase voice mail.

WAN

Red de Área Ancha

Red de comunicaciones que cubre amplias áreas geográficas, como provincias, distritos y países.

World Wide Web o WWW

Es el servicio de Internet más difundido, se caracteriza por la utilización de documentos WWW, que se enlazan con otros documentos WWW por medio de HIPERTEXTO (técnica de enlace de texto), el cual enlaza los documentos con solo hacer un clic con el mouse (ratón).

INDICE DE ANEXOS

1. PLAN DE CONTINGENCIAS.
2. DESCRIPCION DE LA UNIVERSIDAD ANDINA NESTOR CACERES
VELASQUEZ.
3. DESCRIPCION DEL SISTEMA DE INFORMACIÓN ADMINISTRATIVO
DE LA U.A.N.C.V.
4. DESCRIPCION DEL SISTEMA DE INFORMACION ACADEMICA.
5. NORMAS GENERALES DEL PERÚ.
6. NORMAS Y DISPOSICIONES DE LA CONTRALORÍA GENERAL DE LA
REPÚBLICA - CGR.
7. NORMAS DEL INSTITUTO NACIONAL DE DEFENSA DE LA
COMPETENCIA Y PROTECCION DE LA PROPIEDAD INTELECTUAL –
INDECOPI.
8. NORMAS DEL INSTITUTO NACIONAL DE ESTADISTICA E
INFORMÁTICA – INEI
9. DESCRIPCION ISACA.
10. NORMAS GENERALES PARA LOS SISTEMAS DE AUDITORÍA DE LA
INFORMACIÓN.

ANEXO N° 01

PLAN DE CONTINGENCIAS

Objetivo General

Evaluar, verificar y comprobar el uso adecuado de los recursos informáticos de la entidad bajo los principios de recuperación del negocio en economía, eficacia, eficiencia y transparencia la misma que se encuentre enmarcado en el cumplimiento de los objetivos y metas trazadas en los planes de la Institución.

Objetivos Específicos

Teniendo entre sus objetivos específicos los siguientes:

- Implementar el proceso que cumpla las políticas, normas y procedimientos institucionales y legales.
- Adecuar el procedimiento para la selección, uso y resguardo de los activos físicos y lógicos.
- Consistenciar los sistemas y de las aplicaciones desarrolladas.
- Asegurar una adecuada y eficaz operación de los sistemas y de las aplicaciones desarrolladas
- Detectar deficiencias en busca de las mejoras en los recursos informáticos que se utilizan en la organización, incluyendo los servicios prestados por terceros y que permitan con el informe final, efectuar acciones preventivas y correctivas para eliminar las fallas y carencias que se detecten.

- Salvaguardar físicamente los equipos de Hardware.
- Verificar y evaluar.
- Proteger los activos de la Organización.

Acciones de Control Programadas

Programa de Auditoría

Específicamente las actividades incluidas en los procedimientos de auditoría para del Área de Sistemas en el Programa de Auditoría deberá tomar en cuenta:

1. Revisar el organigrama de la Institución y del área de sistemas
2. Revisión de archivo permanente o auditorías anteriores realizadas por los Organos de Control
3. Revisión de información obtenidos de la entidad (archivo permanente de Auditoría de Sistemas)
4. Medir en forma preliminar el riesgo tecnológico
5. Evaluar los recursos humanos del área de sistemas
6. Revisar el plan estratégico de sistemas para identificar las modificaciones a sistemas existentes y el desarrollo de sistemas nuevos
7. Revisar la plataforma tecnológica
8. Hardware
9. Servidores de datos, Servidores de Aplicaciones, Comunicaciones, etc.
10. Microcomputadoras, terminales, periféricos, etc.
11. Sistemas Operativos

12. Software de desarrollo
13. Software de productividad
14. Software aplicativo
15. Software base
16. Revisar el plan anual de auditoría de sistemas notando las auditorías que se debieron realizar
17. Obtener y revisar informes de auditorías realizadas e identificar observaciones no superadas así como áreas con problemas
18. Revisar el manual de estándares de desarrollo y programación
19. Revisar las políticas, procedimientos de control y mantenimiento de sistemas
20. Revisar el plan de seguridad física y el plan de contingencias
21. Obtener y revisar flujogramas de los sistemas a ser examinados
22. Revisar los controles y procedimientos escritos
23. Revisar las políticas y estándares para microcomputadoras y redes
24. Revisar copias de los contratos, convenios, adjudicaciones y licitaciones relacionadas con la adquisición, desarrollo y mantenimiento de hardware y software.

Procedimiento de Auditoría

Se especificara los pasos a seguir por la Comisión de Control, antes, durante y después del proceso de auditoría.

a. Antes

- Anuncio, Reuniones Iniciales.
- Documento de Presentación (Acreditación).
- Reuniones iniciales.
- Motivo del Examen y Alcance.

b. Durante

- Investigación.
- Entrevistas, Reuniones.
- Validación de hechos.
- Observaciones y recomendaciones.
- Reporte final en los papeles de trabajo.

c. Después

- Reunión Final.
- Planes de acción para seguimiento.
- Seguimiento.

PROGRAMA DE AUDITORIA

El programa de auditoría comprende una relación ordenada de procedimientos a ser aplicados durante la auditoría, que permitan obtener las evidencias competentes y suficientes para alcanzar el logro de los objetivos establecidos. El auditor se apoya en

estos procedimientos para establecer la naturaleza, oportunidad y alcance de los procedimientos a aplicar, por lo que deberá tomar en cuenta lo siguiente:

- Se desarrollan a partir del conocimiento de la Organización y sus recursos informáticos.
- Su flexibilidad debe permitir modificaciones, mejoras y ajustes que a juicio del Jefe de Comisión y Supervisor se consideren pertinentes durante el proceso de la auditoría.
- Guían la acción del auditor y sirven como elemento para el control de la labor realizada.
- Permite también la evaluación del avance del examen y la correcta aplicación de los procedimientos.
- Debe ser lo suficientemente detallado de manera que sirva como guía y como medio para controlar la adecuada ejecución del trabajo.

La responsabilidad de la elaboración de los respectivos programas corresponde al Jefe de Comisión y al Supervisor de la Comisión. En el proceso de preparación, también se debe considerar el riesgo tecnológico de la Entidad.

Específicamente las actividades incluidas en los procedimientos de auditoría para del Área de Sistemas en el Programa de Auditoría deberá tomar en cuenta:

1. Revisión del organigrama de la Institución y del área de sistemas.
2. Revisión de archivo permanente o auditorías anteriores realizadas por los Organos de Control.
3. Revisión de información obtenidos de la entidad (archivo permanente de Auditoría de Sistemas).
4. Medir en forma preliminar el riesgo tecnológico.
5. Evaluar los recursos humanos del área de sistemas.
6. Revisar el plan estratégico de sistemas para identificar las modificaciones a sistemas existentes y el desarrollo de sistemas nuevos.
7. Revisión de la plataforma tecnológica.
8. Hardware.
9. Servidores de datos, Servidores de Aplicaciones, Comunicaciones, etc.
10. Microcomputadoras, terminales, periféricos, etc.
11. Sistemas Operativos.
12. Software de desarrollo.
13. Software de productividad.
14. Software aplicativo.
15. Software base.
16. Revisar el plan anual de auditoría de sistemas notando las auditorías que se debieron realizar.
17. Obtener y revisar informes de auditorías realizadas e identificar observaciones no superadas así como áreas con problemas.
18. Revisar el manual de estándares de desarrollo y programación.

19. Revisar las políticas, procedimientos de control y mantenimiento de sistemas.
20. Revisar el plan de seguridad física y el plan de contingencias.
21. Obtener y revisar flujogramas de los sistemas a ser examinados.
22. Revisar los controles y procedimientos escritos.
23. Revisar las políticas y estándares para microcomputadoras y redes.
24. Revisar copias de los contratos, convenios, adjudicaciones y licitaciones relacionadas con la adquisición, desarrollo y mantenimiento de hardware y software.

PROGRAMA DE AUDITORIA PARA REDES TCP/IP E INTERNET

Objetivo:

Verificar los controles relativos a redes que usan TCP/IP e Internet para asegurar que:

- a. Los activos físicos son salvaguardados adecuadamente
- b. El software y los archivos de datos son asegurados adecuadamente
- c. Los soportes técnicos y administrativos son adecuados
- d. El soporte administrativo y el conocimiento del sistema de telecomunicaciones son adecuados

Trabajos a realizar

- I. Obtener la siguiente documentación:
 - A. Diagramas de WAN, mostrando todas las ubicaciones de la red incluyendo los métodos usados de transmisión en el WAN (x.25, frame-relay, t-1, dial-up, etc.)
 - B. Diagramas detallados de red para todas las redes de área local dentro del alcance de la auditoría, que incluyan todos los nodos significativos, como ruteadores, firewalls, gateways, servidores de archivo, sistemas de proceso del host (Unix, mainframe, etc.), con direcciones de red y nodos IP y métodos de enlace y transmisión (ethernet, token ring, tec)
 - C. Descripción narrativa de aplicaciones significativas en uso acompañando las descripciones de servicios de TCP/IP (telnet, ftp, nfs, tftp, etc.) necesario para soportar estas aplicaciones.

- D. Listados de archivos de control de la red para sistemas significativos dentro el alcance de la auditoría (/etc/inetd.conf,/etc/host.equiv,/etc/exports, etc.)
- E. Listados de archivos de configuración de ruteadores que conectan a redes externas o son usados para segmentar redes de servidores de red o usuarios.
- F. Listados de archivos de configuración de firewall y archivos de carga (scripts)
- G. Organigramas y descripción de trabajos para el personal de soporte de la red
- H. Políticas y procedimientos de operación y seguridad de la red

Seguridad física

Determinar que está implementada en la red una adecuada seguridad física sobre los medios de transmisión y dispositivos de red de manera tal que prevengan el acceso no autorizado y/o las modificaciones a sistemas y datos. Revise los diagramas del WAN para identificar redes y direcciones con sistemas host significativos. Evaluar la seguridad de estos centros de operación.

- II. Obtener diagramas de cableado y conectividad de la red dentro del alcance de la revisión y realiza las siguientes tareas:
 - A. Revise los diagramas de cableado de las estaciones de trabajo. Observe el cableado para determinar que las estaciones de trabajo están protegidas de interferencia de otros sistemas o dispositivos, lo cual puede degradar la calidad de transmisión.

- B. Determine que las bocas de conexión del cableado y concentradores están ubicados en áreas de seguridad accesibles solo a personal de soporte de la red.
 - C. Observe el centro de operación del sistema y la red para determinar que el acceso físico es otorgado sobre la base de ‘como se necesite’ y que esté bien controlado.
 - D. Determine que software de administración de red está siendo usado para monitorear las conexiones físicas a la red y estimar la carga de tráfico.
 - E. Observe y evalúe los controles de acceso físico sobre los satélites y antenas de transmisión de microondas, para determinar que el acceso está restringido.
- III. Revise el diagrama de cableado y compare con las conexiones físicas, observando la etiquetación de bocas de conexión, enlaces de multiplexores, modems, etc., para asegurar que todas las conexiones físicas están autorizadas y documentadas.

Seguridad TCP/IP en los niveles de encadenamiento (OSI - ISO)

Determinar que los objetivos de seguridad de los niveles de encadenamiento están siendo adecuadamente cumplidas.

- I. Usando los diagramas de red, identificar los protocolos de encadenamiento del LAN (ethernet, token ring, etc.) y los protocolos de encadenamiento del WAN (x.25, frame relay, T - 1, etc) en uso.

- A. Evaluar la necesidad de filtros de seguridad de puentes (bridges) en direcciones encadenadas para proteger porciones confidenciales en la red
 - B. Determinar si la encriptación del nivel de encadenamiento es necesario y es propiamente usado para proteger transmisiones a través de encadenamientos entre LANs y WAN públicos.
- II. Identificar todos los encadenamientos y protocolos dial - up en uso (SLIP,PPP)
- A. Para encadenamientos SLIP (serial link interfase protocol), determine si el método de autenticación PAP (password authentication protocol) está suplementado por procedimientos que aseguren que los passwords son cambiados con regularidad, formatos están registradas en el dial - up, se registre accesos al servidor, y estos registros sean revisados regularmente.
 - B. Para encadenamientos PPP (point - to - point protocol), determine que autenticación CHAP (challenge - handshake authentication protocol) está siendo usada
 - C. Si autenticaciones Tacacs están siendo usadas para soportar la seguridad de acceso remoto, revise la efectividad de la configuración de Tacacs y los controles de acceso físico y lógico sobre el servidor de seguridad Tacacs.

Seguridad de los niveles de la red

Determinar que transmisiones a través de la red son enviadas propiamente y en forma segura a sus destinos autorizados a través de rutas autorizadas.

- I. Obtener un diagrama detallado de las redes, incluyendo redes y direcciones de nodos IP y nombres autorizados de host. (DSN names) y:
 - A. Determinar si las direcciones IP son legales y los nombres DNSS están siendo usados y si la organización están siguiendo una identificación (poner nombres) bien organizada de direcciones IP y esquemas de sub-red para prevenir duplicidad de direcciones IP en el host y la red.
 - B. De una estación de trabajo de red en cada red significativa, use el utilitario de seguimiento de ruta (tracert en Windows 95) para documentar la ruta de la red de la estación de trabajo a varios de los nodos listados en la documentación del "tracert command" (nombre del host o dirección IP). Compare la salida del "tracert command" con la documentación de la red para asegurar que la documentación de la red está actualizada en cuanto a ruteadores y sistemas en la ruta de la red. Investigue cualquier ruta no documentada o nodos intermedios que no son ruteadores.
 - C. También usando el utilitario de seguimiento de ruta, siga la ruta a sistemas host inalcanzables para determinar si el límite máximo de saltos entre nodos (hops) está activo (el máximo usualmente 30).

- D. Use el utilitario PING para probar la exactitud de la dirección IP y los nombres host del sistema listados en los diagramas y documentación del sistema por el PING (nombre de host o dirección IP). Investigue y resuelva cualquier sistema que no responda.
 - E. Obtener un account para los sistemas host significativos. Ingrese y ejecute el comando `netstat -rn` y `netstat -r` para listar la tabla de rutas par ese nodo por nombre del sistema (-n) y dirección IP (-r). Compare la salida de este comando con la documentación de la red par asegurar la exactitud de la documentación de la red para asegurar la exactitud de la documentación. (en sistemas unix).
- II. Identifique todos los ruteadores que conecta la red a una red externa, o a una red manejada por otra organización y los ruteadores que conectan el sistema host ay las redes de servidores a redes de usuarios y redes externas. Obtenga impresos de los archivos de configuración de la red y realice lo siguiente:
- A. Determine que el paquete de actualización de tablas de ruta IGP y EGP (usado para ruteo dinámico) están filtrados y descargados para prevenir que ellos entren en la red interna.
 - B. Determine si las actualizaciones de IGP y EGP están desactivadas y si existen procedimientos efectivos para asegurar la exactitud de las tablas de ruteo estático.
 - C. Determinar si los ruteadores tienen definido rutas estáticas que permitan el paso de tráfico de solo ruteadores especificados en la conexión externa

de la red (usualmente el caso cuando se conecta a una red de vendedor, afiliada o de negocios, etc.)

- D. Revise la configuración para asegurar que paquetes usando la opción de ruta fuente suelta (loose source routing OFF), son filtrados y descargados para prevenir el ingreso a la red interna.
- E. También revise el archivo de configuración de ruteador para asegurar que el ruteador ignora mensajes de redirección ICMP (ICMP OFF), los cuales pueden ser usados para cambiar la tabla de ruteo.
- F. Asegúrese que una regla de filtrado ha sido implementada para detectar paquetes de interfaces externas que tienen una dirección fuente IP de un sistema de la red interna (detecta dirección IP spoofing)

III. Revise y evalúe la administración de ruteadores y controles de acceso para todos los ruteadores, especialmente aquellos ruteadores que conectan la red a una red externa o una administrada por otra organización, y ruteadores los cuales conectan el sistema host y los servidores de red a usuarios externos de la red y redes externas. Obtenga una impresión de los archivos de configuración de los ruteadores y efectúe lo siguiente:

- A. revise y evalúe controles administrativos sobre acceso de usuarios y mantenimiento de ruteadores (work request, actualización de sistemas operativos, sign - offs (salidas), etc.).

- B. Revise los procedimientos de backup para asegurar que la configuración es respaldada y asegurada y es reinstalada para subsecuentes actualizaciones de sistemas.
- C. Determine que todo telnet y puerto e acceso a consola están protegidos por password, por el password del tuteurador o métodos de autenticación Tacacs.
- D. Asegúrese que todos los passwords están almacenados en forma encriptada usando un algoritmo seguro de encriptación.
- E. Determine si el acceso Telnet a los ruteadors ha sido completamente desactivado en ruteadors que se conectan a redes externas. (En la mayoría de los casos deber ser desactivado para aminorar el riesgo de acceso Telnet de redes externas).
- F. Evaluar la otorgación adecuada de privilegios de acceso para modificar el archivo de configuración de ruteadors.
- G. Si Tacacs es usado, revise la seguridad del sistema operativo sobre el servidor Tacacs; también asegúrese que los controles administrativos y los controles de respaldo sobre la base de datos de autenticación de Tacacs es adecuado.
- H. Revise accesos SNMP al ruteador para asegurar que los valores de configuración SNMP (sets) están restringidos a estaciones de trabajo de control autorizadas y que el password comunitario ha sido cambiado de su valor por omisión a valores de mayor seguridad y confidencialidad.

**PROGRAMA DE AUDITORIA PARA LA VERIFICACIÓN
DE LA BASE DE DATOS**

I. Obtener la siguiente documentación y accesos:

- a. La política para seguridad de computadoras.
- b. Definiciones de los puestos de:
 - 1. Administradores de seguridad.
 - 2. Administradores de bases de datos.
- c. El inventario de aplicaciones que usan las bases de datos.
- d. Listas del contenido de los archivos que dan acceso y permisos a los usuarios.
- e. Los procedimientos para administrar programas de seguridad tal como ACF2, RACF O Top Secret.
- f. Una palabra clave con autorización para revisar los archivos de seguridad y control de acceso del sistema.

II. Revisar la política de seguridad para determinar si:

- a. La política está escrita y ha sido comunicado a todos los usuarios (empleados, consultores, etc.).
- b. La política establece que todos los datos son la propiedad de la entidad y que no pueden ser revelados o modificados sin permiso específico.
- c. La política da autoridad y responsabilidad suficiente al oficial de seguridad para permitir un nivel adecuado de seguridad.

- d. La política establece la responsabilidad para la determinación y otorgación de permisos de acceso.
- e. La política defina claramente los tipos de acceso que son y no son apropiados.
- f. La política requiere autorización escrito para obtener acceso.

III. Control de acceso - Determinar si los siguientes controles existen:

- a. El sistema de seguridad (ACF2, RACF, o Top Secret) requiere el uso de códigos de identificación de usuarios (userids) y palabras claves para entrar en la base de datos.
- b. Hay coordinación de códigos de identificación de usuarios entre sistemas y plataformas
- c. Los códigos de usuarios terminados están borrados del sistema.
- d. Si existe un código de usuarios visitantes, ¿Por qué existe? ¿Qué tipos de permisos tiene el código?

IV. Respaldo - Determinar si los siguientes controles existen:

- a. Existen políticas y procedimientos para hacer copias de respaldo de las bases de datos.
- b. Los operadores tienen instrucciones escritas que explican como y cuando hacer las copias de respaldo.
- c. Un administrador revisa el respaldo y el uso del respaldo para asegurar que es apropiado.

PROGRAMA DE AUDITORÍA PARA COMUNICACIONES

- Verificar que la Institución establezca políticas, procedimientos y controles que minimicen los riesgos sobre la seguridad de datos y de acceso no autorizado, presentes en la utilización de las telecomunicaciones para la distribución de la información y ejecución remota de procesos.

- Verificar la existencia de controles para asegurar la confiabilidad, seguridad y continuidad de la red de comunicaciones, que incluyan por lo menos:

- **Seguridad de terminales:**

Restricciones de acceso físicos a las terminales y controles de sistemas por función, operador, tipo de transacción y datos, etc.;

- **Registro de actividad de la red:**

Intentos no autorizados para acceder a un sistema o a niveles no autorizados para el usuario y archivo de transacciones;

- **Acceso restringido:**

Restricciones de acceso a personas ajenas a la red por medio de sistemas remotos de telecomunicación; y

- **Transmisión de datos:**

Rara proteger confidencialidad y precisión de datos transmitidos.

PROGRAMA DE AUDITORIA PARA LA EVALUACIÓN DEL DESARROLLO DE SISTEMAS

I. PARA LA ETAPA DE ANALISIS DE SISTEMAS

El objetivo inicial es asegurar que el equipo del proyecto ha establecido la necesidad para el sistema y determinado que su costo es menor o igual a sus beneficios.

I.1 Información requerida

- a. Revisar la metodología para el diseño de sistemas.
- b. Revisar la metodología usada para medir costos y beneficios.
- c. Revisar los reglamentos, políticas y procedimientos por el área por la cual están desarrollando el sistema.

I.2 Tener la documentación preparada en esta fase del proyecto

- a. Estudio de factibilidad.
- b. Análisis de riesgos.
- c. Análisis de costos y beneficios.
- d. Informe de la fase.

I.3 Determinar si el estudio de factibilidad identifica el problema y justifica su solución

- a. Determinar si los usuarios y sus departamentos han sido identificados.

- b. Determinar si la descripción de la necesidad para el sistema.
- c. Determinar si los objetivos del proyecto han sido claramente definidos para que puedan servir como base para medir la efectividad del sistema durante y después del proceso de desarrollo del sistema.
- d. Determinar si los usuarios han participado en esta fase.
- e. Determinar si los riesgos del sistema han sido analizados.
- f. Determinar si el análisis de costos y beneficios incluye todos los aspectos relacionados al desarrollo, operación y mantenimiento del sistema.
- g. Determinar si los gerentes responsables, y la alta dirección, han revisado y aprobado el estudio y la recomendación antes de la iniciación de la siguiente fase.

II. PARA LA ETAPA DE DISEÑO LOGICO PRIMERA PARTE

El objetivo es verificar que las necesidades de los usuarios fueron convertidos a requerimientos del sistema, que el diseño incluye los controles necesarios, y que el diseño está de acuerdo con los estándares.

II.1 Revisar la documentación preparada en esta fase anterior del proyecto:

- a. Estudio de factibilidad.
- b. Análisis de riesgos.
- c. Análisis de costos y beneficios.
- d. Informe de la fase.

II.2 Recopilar la documentación preparada en esta fase del proyecto incluyendo el programa de trabajo de la fase.

II.3 Determinar si el programa de trabajo incluye:

- a. La estrategia para la administración y el control de la fase.
- b. Metas y actividades para la fase y las subfases.
- c. Una estimación de los recursos necesitados en la fase.
- d. Puntos de revisión y aprobación en la fase.
- e. Métodos de análisis, documentación, reportaje de problemas, administración de cambios, y aprobación.
- f. La identificación de herramientas disponibles.

II.4 Revisar la documentación que defina las necesidades funcionales del sistema para determinar si incluye:

- a. Una definición de los objetivos del nuevo sistema.
- b. Una descripción de los procesos y procedimientos actuales.
- c. Una descripción de los procesos y procedimientos del nuevo sistema.
- d. Un resumen de los mejoramientos y efectos (impactos) esperados.
- e. La identificación de entradas, datos internos, y salidas del nuevo sistema.
- f. Las funciones que el nuevo sistema va a realizar.
- g. Los requerimientos de comportamiento del nuevo sistema (tiempo de respuesta, etc.).
- h. Los planes de recuperación de errores y desastres para el nuevo sistema.

- i. Una definición de las necesidades de hardware y software para el nuevo sistema.
- j. Una descripción del flujo de datos por un nuevo sistema desde la iniciación de las transacciones hasta las salidas finales y su distribución a usuarios.
- k. Una descripción de las interfaces con otros sistemas.
- l. Una descripción de requerimientos de seguridad y confidencialidad en el nuevo sistema.
- m. Una descripción de los controles necesarios para el sistema.
- n. El plan para el desarrollo del sistema (la siguiente fase).

II.5 Determinar si existe una definición detallada de requerimientos de información

- a. Verificar que la definición de requerimientos permitirá la definición de datos de prueba.
- b. Realizar entrevistas con usuarios para determinar si los requerimientos son
- c. razonables y completos.
- d. Verificar que los requerimientos son consistentes con estándares para datos (diccionario de datos y administración de bases de datos).

II.6 Verificar que la definición de entradas incluye:

- a. Requerimientos para la validación y verificación de datos.
- b. Medidas para asegurar la seguridad y confidencialidad de datos.
- c. Reglas para definir y autorizar transacciones.

- d. Procedimientos para establecer totales de controles (controles de lotes).
- e. Practicas para autorización de entradas y actualizaciones.

II.7 Verificar que la definición de archivos y bases de datos incluye:

- a. Definiciones de formatos y formas de organización de archivos.
- b. Relaciones entre datos en bases de datos (esquema y sub esquema).
- c. Tamaños de archivos y bases de datos.
- d. Medidas para asegurar la seguridad y confidencialidad de datos.

II.8 Verificar que la definición de procesos incluye:

- a. Requerimientos de validación.
- b. Requerimientos de interés.
- c. Requerimientos de oportunidad y tiempo de procesamiento.
- d. Requerimientos de flexibilidad.

II.9 Verificar que la definición de salidas incluye:

- a. Contenido y formato de salidas.
- b. Autorización de usuarios para recibir salidas.
- c. Periodos de retención de salidas
- d. Existencia y senderos de auditoría.

II.10 Determinar si los usuarios, los gerentes responsables, y la alta dirección, han revisado y aprobado el diseño lógico del sistema y la recomendación de seguir adelante con el proyecto antes de la iniciación de la siguiente fase.

III. PARA LA ETAPA DE DISEÑO LOGICO SEGUNDA PARTE

III.1 Han desarrollado especificaciones para el sistema, los subsistemas y cada programa que incluyen la siguiente:

- a. Descripción narrativa.
- b. Definición de las funciones.
- c. Requerimientos de comportamiento.
- d. Configuración necesaria de hardware.
- e. Software de sistema necesario.
- f. Interfaces con otros sistemas.
- g. Requerimientos de seguridad y confidencialidad.
- h. Controles operacionales.
- i. Técnicas de control de la aplicación y de auditoría.
- j. Flujo del sistema (incluyendo un flujograma del sistema).
- k. Requerimientos de archivos y bases de datos (tamaño).

III.2 Las especificaciones para programas incluye:

- a. Controles para y dentro del programa.
- b. Diccionario de data.
- c. Procedimientos de operación.
- d. Formatos de las entradas.
- e. Definición de la lógica del programa.
- f. Formatos de las salidas.
- g. Definiciones técnicas de los archivos y las bases de datos.

III.3 Las especificaciones de los archivos y las bases de datos

- a. Identificación.
- b. Sistemas.
- c. Estructura física.
- d. Estructura lógica.
- e. Software para mantener la unidad.
- f. Controles de accesos.
- g. Procedimientos para hacer copias de respaldo.

III.4 Verificar que el equipo ha preparado un plan para la aprobación del sistema y entrenamiento de los usuarios.

El plan de aprobación existe e incluye

- 1. Objetivos.
- 2. Alcance.

3. Procedimientos.
4. Especificaciones y descripciones de todas las pruebas, incluyendo datos de prueba.
5. Metodología para revisar los resultados.

IV. PARA LA ETAPA DE IMPLEMENTACION

IV.1 Un manual de usuarios ha sido desarrollado que incluye por lo menos los siguientes elementos:

- a. Descripción narrativa.
- b. Flujograma del sistema.
- c. Descripción de hardware y software necesario.
- d. Estructura y función de cada componente del sistema.
- e. Descripciones de todos los archivos y bases de datos.
- f. Descripciones de las entradas.
- g. Requerimientos y procedimientos para la entrada de datos.
- h. Descripción del flujo de los datos por el sistema.
- i. Descripciones de las salidas.
- j. Procedimientos para usar el sistema.
- k. Instrucciones para responder a mensajes de errores.

IV.2 Un manual de operaciones ha sido desarrollado que incluye por lo menos

los siguientes elementos:

- a. Flujograma detallado del sistema.
- b. Secuencia de operaciones.
- c. Inventario de programa.
- d. Inventario de archivos y bases de datos.
- e. Lista de las configuraciones de los programas para diferentes corridas.
- f. Descripción de interfaces entre programas.
- g. Código (JCL) necesario para cada corrida.
- h. Instrucciones para los operadores.
- i. Fuentes de entradas y salidas por cada programa.
- j. Lista de salidas con destinos.
- k. Procedimientos de recuperación.
- l. Procedimientos de emergencia.
- m. Procedimientos de respaldo.
- n. El manual de operaciones no debe incluir:
 1. Diagramas o documentación de la lógica de los programas.
 2. Listas del código.

IV.3 Un manual de mantenimiento del sistema ha sido desarrollado que incluye por lo menos los siguientes elementos

- a. Descripción detallada de cada programa en el sistema.
- b. Hardware y software necesario por el sistema.

- c. Descripciones detalladas de los archivos y las bases de datos.
- d. Diagramas o documentación de la lógica de los programas.
- e. Listas del código de cada programa.
- f. Lista d códigos de errores, sus causas y procedimientos para corrección de los errores.

IV.4 Un programa de entrenamiento ha sido desarrollado que incluye por lo menos los siguientes elementos:

- a. Identificación de los participantes.
- b. Identificación de los instructores.
- c. Horario para los cursos de capacitación.
- d. Resumen de los objetivos y conceptos.
- e. Presupuesto para capacitación.

IV.5 Un programa de calidad total ha sido desarrollado que incluye por lo menos los siguientes elementos:

- a. Revisión del código por terceros.
- b. Aprobación del código por el gerente del proyecto.

IV.6 Un programa de conversión ha sido desarrollado que incluye por lo menos los siguientes elementos:

- a. Plan de conversión de datos.
- b. Plan de post-conversión auditoría de archivos y bases de datos.
- c. Plan de conversión del sistema.
- d. Plan de post-conversión auditoría del sistema

ANEXO N° 02

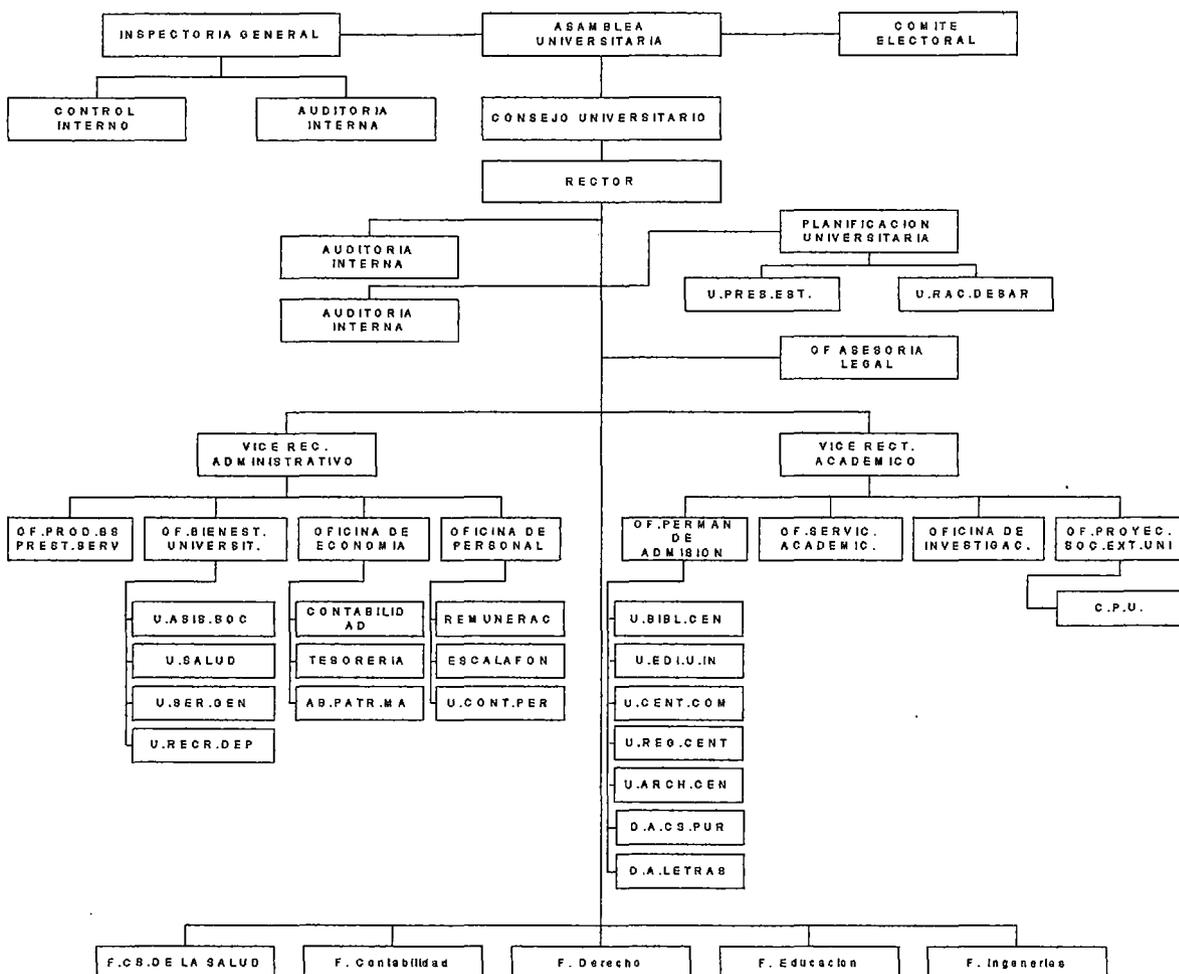
DESCRIPCION DE LA UNIVERSIDAD ANDINA

NESTOR CACERES VELASQUEZ

Información Introductoria

Breve reseña de la Entidad y de la capacidad operativa del Organismo de Auditoría Interna de la Entidad.

1. ORGANIGRAMA DE LA UNIVERSIDAD ANDINA NESTOR CACERES VELASQUEZ DE JULIACA



2. ESTRUCTURA ORGANIZATIVA

ORGANOS DE GOBIERNO	Asamblea Universitaria Consejo Universitario Consejo de Facultad
ORGANOS DE LA ALTA DIRECCION	Rectorado Vice-Rectorado Académico Vice-Rectorado Administrativo
FACULTADES	<p>FACULTAD DE CIENCIAS DE SALUD C.A.P. de Obstetricia C.A.P. de Obstetricia C.A.P. de Obstetricia</p> <p>FACULTAD DE CS CONTABLES Y ADMINIST. C.A.P. de Contabilidad C.A.P. de Administración y Marketing</p> <p>FACULTAD DE INGENIERIAS Y CS PURAS C.A.P. de Ingeniería Civil C.A.P. de Ingeniería de Sistemas C.A.P. de Ingeniería Comercial e Industrial C.A.P. de Ingeniería Mecánica Eléctrica</p> <p>FACULTAD DE CS JURIDS Y POLITICAS C.A.P. Profesional de Derecho</p> <p>FACULTAD DE CS DE LA EDUCACION C.A.P. de Educación Educación Primaria Educación Secundaria, en la de: Ciencias Sociales Bioquímica Físico Matemática W. Lengua, Literatura, Filosofía y Psicología.</p>

<p>DEPARTAMENTOS ACADEMICOS</p>	<p>Departamentos Académicos de Ciencias Departamentos Académicos de Letras</p>
<p>ORGANOS DEL RECTORADO</p>	<p>Secretaría General Oficina de Planificación Universitaria Oficina de Asesoría Legal Oficina de Imagen Institucional</p>
<p>ORGANOS DEL VICE-RECTORADO ACADEMICO</p>	<p>Oficina Permanente de Admisión Oficina de Servicios Académicos Oficina de Investigación Prod. De Bs Prestación de Servicios. Oficina de Proyección Social, Extensión y Bienestar Universitario.</p>
<p>ORGANOS DEL VICE-RECTORADO ADMINISTRATIVO</p>	<p>Oficina de Economía Oficina de Personal</p>
<p>ORGANOS AUTONOMOS</p>	<p>Organo de Inspección y Control Interno Tribunal de Honor Comité Electoral</p>

3. Estructura de Cargos

Rector de la UANCV:

Mg Germán Rivera Olivera

Vice-Rector Académico :

Abog. Justo Sosa Arohuanca

Vice-Rector Administrativo :

Eco. Héctor Arapa Yapo

Secretaria General :

Prof. Pascual Huacasi Sucasaca

Planificación Universitaria :

Eco. Fredy Molina Narváez

Oficina Asesoría Legal :

Abog. Andrés Cansaya Machaca

Organo de Control Interno :

Abog. Ricardo Cuba Salerno

Oficina de Imagen Institucional :

Abog. Braulio Gonzales Lima

Oficina de Servicios Académicos :

Prof. Gerardo Gallegos Sanchez

Oficina de Bienestar Universitario y Extensión Social :

Prof. Pedro Lanza Castro

Oficina de Personal :

Prof. Walter Herrera

Oficina de Economía:

CPC Obdulio Collantes M.

Oficina de Contabilidad :

CPC Juan Zea Pérez

Oficina de Investigación :

Lic. Adm. Elida Sueldo Arriaga

Oficina de Cómputo e Informática:

Ing. Elías Lizarraga Armaza

Centro de Pre Universitario:

Ing. Cristóbal Apaza Pacori

Instituto de Informática:

Ing. Marco Antonio Quispe Barra

DECANOS :

Decano de la Facultad de Cs de la Salud

Méd. Fredy Andía Angulo

Decano de la Facultad de Cs Jurídicas y Políticas

Abog. Guillermo Valdez Pineda

Decano de la Facultad de Cs de la Educación

Prof. Luis Otto Guerra Pacheco

Decano de la Facultad de Ingeniería y Cs Puras

Ing° Cesar Camargo Nájjar

Decano de la Facultad de Cs Contables y Administraciones

Lic. Hugo Barrantes Sánchez

Representantes Estudiantiles:

- Gilber Sánchez Sosa
- Edwin Martínez Soto
- Isabel Parisaca Chávez
- Germán Sanca Pacori
- Richard Condori Cruz

Representantes Graduados:

Lic Biondi Oviedo Villegas

Representante Fundación Patrocinadora:

Abog. Braulio González Lima

DOCENTES PRINCIPALES

Abog. Luis G. Valdez Pineda

Ing°. Fabián Vilca Medina

Méd. Hubert Oporto Malaga

Prof. Rubén Sosa Flores

Prof. Gerardo Gallegos Sánchez

Soc. Raúl Niño de Guzmán Pino

Prof. Moisés Colquehuanca Yujra

Biol. Justina Madariaga Chura

DOCENTES ASOCIADOS

Ps. Luz Paula Diaz Polanco

Lic. Adm. Elida Sueldo Arriaga

Ing. Raúl Ninasivincha Gárate

Ing. Julio Huamán Meza

Prof. Pascual Huacasi Sucasaca

DOCENTES AUXILIARES

Ing° Felipe Charaja Cutipa

Prof. Héctor Moreno Terán

Lic. Alberto Estrada Rospigliosi

TERCIO ESTUDIANTIL

Lizardo Rojas Bustinza

Roger Tumi Tito

Rosa Coyla Carreño

Soledad Monteagudo Apaza

Jackeline Cari Mamani

Vidal Navarro Osorio

Juan Cutipa Condori

Américo Gutierrez Pineda

Yesenia Caballero Aliaga

Julia Urviola Salazar

Edgar Mamani Cahuina

Pablo Arce Vilca

Richard Zegarra Coaguila

Rosbelu Laura Coaquira

4. Gestión Económica y Financiera

El presupuesto de la Universidad Andina “Néstor Cáceres Velásquez” para el semestre de 1998-2, fue de S/. 3’878,532, para el semestre 1999-1 el presupuesto representó S/. 3’972,146, presentando un incremento del semestre 98-2 a 99-1 de 2.41%.

Las pensiones de enseñanza se constituyeron en la principal fuente de ingresos que representó el 87% y para gastos de inversión 13% promedio.

El balance general al 31 de diciembre de 1998, nos indica que el activo total es de S/. 10854,261.75 nuevos soles, esta formado por las cuentas del activo no corriente 52%, principalmente por las cuentas de activos reales inmuebles maquinaria y equipo S/ 6’690,130.26 nuevos soles.

EJECUCIÓN DE GASTOS POR UNIDAD ORGÁNICA AÑO 1998

CTA	GLOSA	TOTAL
941.00	DIRECCION EJECUTIVA – ANTERIOR	74,774.57
941.01	ASAMBLEA UNIVERSITARIA	5,862.32
941.02	COMITÉ ELECTORAL	426.06
941.03	ORGANO DE INSPECCION Y CONTROL	21,628.66
941.04	UNIDAD DE CONTROL INTERNO	13,325.23
941.05	UNIDAD DE AUDITORIA INTERNA	1,053.18
941.06	CONSEJO UNIVERSITARIO	21,527.45
941.07	RECTORADO	82,511.00
941.08	SECRETARIA GENERAL	58,560.86
941.09	OFICINA DE IMAGEN INSTITUCIONAL	74,340.10
941.10	OFICINA DE PLANIFICACION	122,392.81
941.11	UNIDAD DE ESTADISTICA Y PPTO	20.00
941.12	UNIDAD DE RACIONALIZACION	122.00
941.13	OFICINA DE ASESORIA LEGAL	40,568.06
942.01	VICE-RECTORADO ADMINISTRATIVO	1'094,744.83
942.02	OFICINA DE PRODUCCION DE BS	11,860.07
942.03	OFICINA DE BIENESTAR. UNIV. PROYECCION	18,073.42
942.07	UNIDAD DE RECREACION Y DEPORTE	264.80
942.08	OFICINA DE ECONOMIA	140,961.38
942.09	UNIDAD DE CONTABILIDAD	6,183.71
942.10	UNIDAD DE TESORERIA	4,051.66

942.11	UNIDAD DE ABASTECIMIENTOS	902.03
942.12	OFICINA DE PERSONAL	270,192.87
942.13	UNIDAD DE ESCALAFON	294.31
942.14	UNIDAD DE CONTROL DE PERSONAL	172.69
942.15	VICE-RECTORADO ACADEMICO	243,939.61
942.16	OFICINA PERMANENTE DE ADMISION	14,137.91
942.17	OFICINA DE SERVICIOS ACADEMICOS	220,144.82
942.18	UNIDAD DE BIBLIOTECA CENTRAL	2,731.00
942.19	EDITORIAL UNIVERSITARIA E IMPRES.	251.49
942.20	UNIDAD DE CENTRO DE COMPUTO	2,494.05
942.21	UNIDAD DE REGISTRO CENTRAL	4,875.57
942.22	UNIDAD DE ARCHIVO CENTRAL	52.21
942.24	OFICINA DE INVESTIGACION	19,606.37
942.25	OFICINA DE PROYECCION SOCIAL	7,328.33
942.26	LOCAL MANUEL NUÑEZ BUTRON	3,647.32
942.27	LOCAL – LA RINCONADA	23,920.10
942.28	INSTITUTO DE INFORMATICA	410.00
944.01	COORDINACION P.E.P.	20,748.98
944.02	COORDINACION P.E.A	5,219.07
950.00	FACULTADES – ANT	827,851.49
950.01	FACULTADES	315,126.57
951.01	CONSEJO DE FACULTAD CS DE LA SALUD	47.50
951.02	DECANATURA	21,739.18

CTA	GLOSA	TOTAL
951.03	C.A.P. OBSTETRICIA	296,914.47
951.04	C.A.P. ENFERMERIA	59,870.95
951.05	C.A.P. MEDICINA VETERINARIA ZOOTECNIA	32,716.22
951.06	C.A.P. OBSTETRICIA – P.E.	77,849.13
952.01	CONSEJO DE FACULTAD CS. CONT. ADM	5.00
952.02	DECANATURA	27,658.96
952.03	C.A.P. ADMINISTRACION Y MARKETING	116,686.99
952.04	C.A.P. CONTABILIDAD	176,007.25
953.01	CONSEJO DE FACULTAD DE INGENIERIAS	47.50
953.02	DECANATURA	29,043.19
953.03	C.A.P. INGENIERIA CIVIL	268,621.03
953.04	C.A.P. MECANICA ELECTRICA	104,997.30
953.05	C.A.P. INGENIERIA COMERCIAL E INDUSTRIAL	27,444.23
953.06	C.A.P. INGENIERIA DE SISTEMAS	113,189.45
953.07	C.A.P. INGENIERIA CIVIL PUNO	49,797.14
953.08	C.A.P. INGENIERIA DE SISTEMAS PUNO	25,117.62
954.02	DECANATURA CS POLITICAS JURIDICAS	25,623.03
954.03	C.A.P. DERECHO	239,122.24
954.04	C.A.P. DERECHO – P.E.P.	82,342.66
955.02	DECANATURA EDUCACION	32,243.08

955.03	C.A.P. EDUCACION	414,087.24
955.04	C.A.P. EDUCACION – P.E.A.	13,581.51
955.05	PROFESIONALIZACION DOCENTE	2,904.00
955.06	COMPLEMENTACION DOCENTE	9,933.28
957.01	SEDE CENTRAL CPU	677.00
960.00	OBRAS – ANT	31,270.20
971.67	CARGAS FINANCIERAS S. CENTRAL	78,626.98
972.67	CARGAS FINANCIERAS PUNO	242.80
973.67	CARGAS FINANCIERAS AYAVIRI	20.00
980.00	SERVICIOS GENERALES –ANT	429.00
990.00	FUNDO YOCARA – ANT	1,130.57
991.26	ALMACEN CENTRAL JULIACA	8,039.83
991.62	CARGAS DE PERSONAL	30.00
991.63	SERVICIOS PRESTADOS POR TERCEROS	13,193.17
991.65	CARGAS DIVERSAS DE GESTION	589.20
992.26	ALMACEN C. GASTOS AGRICOLAS	3,620.10
992.63	SERVICIOS PRESTADOS POR TERCEROS	1,120.00
992.65	CARGAS DIVERSAS DE GESTION	45.00
993.26	ALMACEN C. GASTOS PECUARIOS	83.00
993.63	SERVICIOS PRESTADOS POR TERCEROS	219.00
993.65	CARGAS DIVERSAS DE GESTION	50.00
	TOTAL	6'164,274.96

BALANCE GENERAL AL 31 DE DICIEMBRE DE 1998

<u>ACTIVO</u>	
<u>ACTIVO CORRIENTE</u>	
CAJA Y BANCOS	S/. 847,453.49
CLIENTES	3'152,057.68
CUENTAS POR COBRAR AL PERSONAL	59,208.35
CUENTAS POR COBRAR DIVERSAS	404,547.44
SUMINISTROS DIVERSOS	30,898.09
CARGAS DIFERIDAS	750,241.42
ANTICIPOS OTORGADOS	344,941.01
TRIBUTOS POR PAGAR	190,769.32
PROVISION COBRANZA DUDOSA	(542,326.57)
	<hr/>
TOTAL ACTIVO CORRIENTE	S/. 5'237,790.23

<u>ACTIVO NO CORRIENTE</u>	
EXISTENCIAS PECUARIAS	S/. 30,100.00
INMUEBLES, MAQUINARIA Y EQUIPO	6'690,130.26
INTANGIBLES	1,572.00
DEPRECIACION Y AMORTIZACION ACUMULADA	(1'105,330.74)
<hr/>	
TOTAL ACTIVO NO CORRIENTE	S/. 5'616,471.52
<hr/>	
TOTAL ACTIVO	S/. 10'854,261.75
 <u>PASIVO</u>	
PASIVO CORRIENTE	S/. 382,963.56
TRIBUTOS POR PAGAR	361,460.65
REM. Y PARTICIPACIONES POR PAGAR	127,854.68
PROVEEDORES	443,053.22
CUENTAS POR PAGAR DIVERSAS	
<hr/>	
TOTAL PASIVO CORRIENTE	S/. 1'315,332.11

<u>PASIVO NO CORRIENTE</u>	
	1'440,494.36
PROVISION PARA BENEFICIOS SOCIALES	
	S/. 1'440,494.36
TOTAL PASIVO NO CORRIENTE	
	434,933.63
PATRIMONIO	4'724,148.95
CAPITAL	542,317.13
CAPITAL ADICIONAL	2'397,035.57
RESULTADOS ACUMULADOS	
RESULTADOS DEL EJERCICIO	
	S/. 8'098,435.28
TOTAL PATRIMONIO	
	S/. 10'854,261.75
TOTAL PASIVO Y PATRIMONIO	

**CAPTACION DE INGRESOS POR PENSIONES DE ENSEÑANZA
Y TASAS POR SERVICIOS EDUCATIVOS**

PARTIDA	TOTAL	%
PENSIONES DE ENSEÑANZA	6,276,965.51	95.38
TASAS POR SERVICIOS EDUCATIVOS	304,154.50	4.62
TOTAL	6,581,120.01	100.00

ENTIDADES ADMINISTRATIVAS:

OBJETIVOS

UNIDAD ORGANICA	OBJETIVOS
VICE-RECTORADO ADMINISTRATIVO	<ul style="list-style-type: none">• Organización el desarrollo de las actividades de Vice-rectorado administrativo.• Organizar el cumplimiento de los objetivos de la universidad.• Coordinar con las oficinas dependientes de Vice-rectorado administrativo.• Transmitir información oportuna entre oficinas.• Adquirir los equipos que se requieren.

UNIDAD ORGANICA	OBJETIVOS
<p style="text-align: center;">BIENESTAR UNIVERSITARIO</p>	<ul style="list-style-type: none"> • Organizar acciones de Bienestar que contribuyen a crear condiciones adecuadas para el cumplimiento de los fines de la Universidad. • Contar con material Bibliográfico disponible (de calidad). • Estudiar y planificar la realidad socio-económica estudiantil. • Brindar servicios médicos y asistenciales a la comunidad Universitaria.

UNIDAD ORGANICA	OBJETIVOS
<p style="text-align: center;">ASISTENCIA SOCIAL, SALUD Y SERVICIOS QUE SE OFRECEN</p>	<ul style="list-style-type: none"> • Formular normas técnicas y directivas tendientes a lograr un eficiente y oportuno cumplimiento de sus funciones. • Promover actividades orientadas a la prevención de enfermedades. • Efectuar el estudio socio económico de estudiante y trabajadores (administrativos y docentes). • Determinar las categorías socioeconómicas para el pago de las tasas educativas. • Brindar apoyo y orientación a los estudiantes para la solución de sus problemas económicos y sociales.

UNIDAD ORGANICA	OBJETIVOS
RECREACION Y DEPORTES	<ul style="list-style-type: none"> • Formular el presupuesto de la unidad en coordinación con el jefe de la oficina. • Programar, organizar, supervisar y controlar la ejecución de actividades deportivas, artísticas y culturales. • Coordinar con los organismos públicos y privados que desarrollan actividades de recreación y deportes. • Presentar informes de la labor realizada durante determinados períodos.

UNIDAD ORGANICA	OBJETIVOS
ECONOMIA	<ul style="list-style-type: none"> • Obtener un sistema contable óptimo, para cumplir eficientemente sus funciones. • Facilitar con rapidez la entrega oportuna de información por parte de otras oficinas. • Contar con personal capacitado para cumplir con sus objetivos. • Contar con personal adecuado en número y calidad e infraestructura adecuada. • Actualizarse en informática y unificarse mediante una red a todas las áreas.

UNIDAD ORGANICA	OBJETIVOS
CONTABILIDAD	<ul style="list-style-type: none"> • Organizar y controlar adecuadamente el sistema de contabilidad. • Llevar adecuadamente la contabilidad de la Universidad emitiendo en su oportunidad los estados financieros. • Tener conexión con las normas del sistema de control. • Asesorar a los diferentes órganos de la Universidad. • Elaborar y registrar la evaluación presupuestal en forma adecuada. • Ordenar en forma adecuada la documentación contable.

UNIDAD ORGANICA	OBJETIVOS
<p style="text-align: center;">TESORERIA</p>	<ul style="list-style-type: none"> • Organizar y mantener en orden los recibos de pagos que faciliten la búsqueda de los mismos, que hayan sido extraviados por los alumnos. • Recepcionar, registrar y controlar los fondos de ingresos y egresos. • Coordinar las acciones inherentes a la administración de fondos con otras oficinas. • Conectarse con la oficina de caja para actualizar estado de cuentas de los estudiantes y otros. • Emitir informes de los movimientos de ingresos y egresos en el tiempo pertinente.

UNIDAD ORGANICA	OBJETIVOS
ABASTECIMIENTO	<ul style="list-style-type: none"> • Elaborar normas y directivas para el funcionamiento de la unidad. • Proponer normas y procedimientos de aplicación institucional en el campo de su competencia. • Supervisar las labores del personal a su cargo. • Coordinar con la oficina de contabilidad.

UNIDAD ORGANICA	OBJETIVOS
PERSONAL	<ul style="list-style-type: none"> • Informar sobre el desempeño del personal administrativo. • Ofrecer eficiencia y eficacia institucional en aspectos técnico administrativos. • Establecer un nexo de concordancia entre el plan institucional con el plan de desarrollo de la Universidad. • Actualización en la oficina de personal. • El personal administrativo debe estar identificado con la Universidad.

UNIDAD ORGANICA	OBJETIVOS
REMUNERACIONES	<ul style="list-style-type: none"> • Entregar en el tiempo establecido la información a economía sobre los resúmenes de descuentos mensuales. • Brindar información oportuna a los trabajadores sobre sus pagos y descuentos hechos en planillas de pagos. • El personal debe dedicarse en forma exclusiva en la elaboración de planillas. • Contar con infraestructura y equipo adecuados.

UNIDAD ORGANICA	OBJETIVOS
ESCALAFON	<ul style="list-style-type: none"> • Rapidez en la absolución de reclamos del personal. • Solicitar información a los docentes de la Universidad acerca de sus historiales o legajos. • Contar con personal capacitado para un buen cumplimiento de sus funciones. • Contar con los equipos adecuados para archivar la información de los docentes y personal administrativo.

UNIDAD ORGANICA	OBJETIVOS
<p style="text-align: center;">CONTROL DEL PERSONAL</p>	<ul style="list-style-type: none"> • Controlar la asistencia del personal docente. • Interesarse por integrarse a la Universidad. • Dedicación a tiempo completo del personal docente a la investigación y capacitación de sus propias carreras académicas.

UNIDAD ORGANICA	OBJETIVOS
<p style="text-align: center;">MANTENIMIENTO Y PRESTACION DE SERVICIOS</p>	<ul style="list-style-type: none"> • Contar con el personal de servicio necesario. • Contar con el material para mantenimiento cuando se le requiera. • Fomentar la dedicación para el y mantenimiento de la Universidad. • Lograr la eficiencia del personal de mantenimiento. • Brindar los servicios de la mejor manera posible.

ENTIDADES ADMINISTRATIVAS:

FUNCIONES

UNIDAD ORGÁNICA DE LA EMPRESA	FUNCIÓN
VICE-RECTOR ADMINISTRATIVO	<ul style="list-style-type: none">• Reemplazar al Rector y/o Vice-Rector Académico en ausencia de los mismos.• Supervisar y coordinar el desarrollo de las actividades económicas, financieras y administrativas.• Preparar normas, técnicas administrativas relacionadas con su ámbito de acción.• Coordinar y controlar el funcionamiento de sus distintas oficinas.• Proponer al Rector del nombramiento del personal administrativo y de servicio permanente o contratado, previa sugerencia de las jefaturas correspondientes.• Formular, coordinar y consolidar los planes, programas y acciones administrativas propuestas por las facultades.

	<ul style="list-style-type: none">• Elevar al Rector a periódica y oportunamente el avance de partidas genéricas y específicas.• Organizar el margen de bienes como muebles e inmuebles controlando que se mantengan actualizados.• Firmar cheques, juntamente con el jefe de la oficina de economía.• Autorizar la adquisición de bienes, prestación de servicios y contratación de obras, cuyos montos serán autorizados por el Consejo Universitario.• Firmar los certificados, constancias y documentos relacionados con el personal juntamente con el jefe de la oficina de personal.• Dictaminar sobre los expedientes relacionados con la función administrativa que provengan de las facultades o de las oficinas administrativas.• Proponer las sanciones del personal administrativo y de servicio, de acuerdo
--	--

	<p>con las propuestas de los jefes de oficina y el reglamento interno correspondiente.</p> <ul style="list-style-type: none">• Preparar los documentos para la elaboración de la memoria del Rector, dentro de su cargo.• Aprobar el proyecto de distribución de aulas en coordinación con el Vice-Rector Académico y la oficina de Planificación Universitaria.• Otras que les sean asignadas por el Rector o el Consejo Universitario.
--	--

UNIDAD ORGANICA	FUNCIONES
<p style="text-align: center;">CENTRO DE PRESTACIÓN DE SERVICIOS.</p>	<ul style="list-style-type: none"> • Proporcionar servicios de transporte local e interprovincial según requerimiento. • Programar el uso de los vehículos de transporte. • Efectuar el mantenimiento y reparación de las unidades móviles. • Formular el presupuesto para el mantenimiento y reparación de las unidades móviles. • Informar sobre las actividades desarrolladas al jefe de oficina. • Otras funciones que le asigne el jefe de oficina.

UNIDAD ORGANICA	FUNCIONES
<p style="text-align: center;">BIENESTAR UNIVERSITARIO.</p>	<ul style="list-style-type: none"> • Promover, organizar, dirigir, supervisar y evaluar programas de previsión de salud, servicio social, recreación y bienestar universitario. • Planificar, dirigir y coordinar la realización de estudios socio-económicos de los estudiantes. • Propiciar y dar las facilidades para la formación de cooperativas de vivienda, producción, consumo y otras que organicen los docentes, administrativos o alumnos. • Promover y facilitar la constitución de clubes integrados por docentes, administrativos, alumno y graduados, para el fomento de las actividades culturales, artísticas, deportivas, de recreación y bienestar. • Coordinar sus acciones con los servicios de salud del Estado, con el Instituto Peruano de Seguridad Social (ESSALUD) y otros organismos afines.

UNIDAD ORGANICA	FUNCIONES
ASISTENCIA SOCIAL	<ul style="list-style-type: none"> • Promover y desarrollar programas de asistencia social para los estudiantes y trabajadores docentes y administrativos de la Universidad. • Formular el presupuesto de la unidad en coordinación con el jefe de oficina y remitirlo a la oficina de planificación universitaria para su consideración. • Buscar el auspicio de las actividades de servicio social, exterior de la Universidad. • Otorgar becas parciales e integrales a los alumnos que efectivamente lo necesiten y demuestren eficiencia académica. • Realizar las visitas domiciliarias a los alumnos que soliciten becas por baja disponibilidad de recursos económicos. • Realizar estudios socioeconómicos de los estudiantes de la Universidad, de igual forma de trabajadores administrativos y docentes.

	<ul style="list-style-type: none"> • Elaborar el plan de trabajo de acuerdo a los recursos disponibles. • Realizar el estudio socio-económico necesarios para la racionalización de becas estudiantiles y para la determinación de las categorías socio-económicas del pago de las tasas educativas. • Proporcionar ayuda y orientación a los estudiantes para la solución de sus problemas económicos sociales. • Tramitar la inscripción y atención de los docentes y no docentes ante el ESSALUD. • Otras que le encargue el jefe de la oficina.
<p style="text-align: center;">SALUD</p> <p style="text-align: center;">y</p>	<ul style="list-style-type: none"> • Proporcionar servicio médico a los miembros de la comunidad universitaria. • Realizar labores de prevención de enfermedades al interior de la Universidad. • Formular normas técnicas y directivas tendientes a lograr un eficiente y oportuno cumplimiento de sus funciones. • Formular el presupuesto de la unidad de coordinación con el jefe de la oficina.

	<ul style="list-style-type: none"> • Promover la realización de charlas, conferencias y exposiciones orientadas a la prevención de enfermedades y otros. • Coordinar sus acciones con los servicios de salud estatal, ESSALUD, y otros organismos afines. • Estudiar las necesidades de equipo y materiales de servicio, proponer al jefe de la oficina las medidas necesarias a ser adoptadas. • Otras que designe la jefatura de bienestar universitario.
<p style="text-align: center;">Servicios que se Ofrecen</p>	<ul style="list-style-type: none"> • Proponer e implementar las normas internas de funcionamiento de los centros de producción de bienes y prestación de servicios. • Implementar los procesos productivos con el fin de obtener una óptima productividad y poner a disposición de los diversos sectores de la comunidad universitarias.

UNIDAD ORGANICA	FUNCIONES
<p style="text-align: center;">RECREACIÓN</p> <p style="text-align: center;">Y</p> <p style="text-align: center;">DEPORTES</p>	<ul style="list-style-type: none"> • Programar, dirigir, organizar, supervisar, controlar, la ejecución de actividades deportivas artísticas y culturales. • Coordinar con los organismos públicos y privados que desarrollan actividades de recreación y deportes. • Realizar programas recreativos vacacionales para estudiantes e hijos de docentes y no docentes. • Responsabilizarse del mantenimiento, materiales, equipos, implementos y muebles que dispone para las actividades recreativas, deportivas y culturales. • Presentar informes periódicos de la labor realizada. • Formular el presupuesto de la unidad en coordinación con el jefe de la oficina. • Fomentar excursiones y organización de círculos culturales, recreativos y de orientación vocacional. • Otras acciones o funciones que le asigne la jefatura.

UNIDAD ORGANICA	FUNCIONES
<p style="text-align: center;">ECONOMIA</p>	<ul style="list-style-type: none"> • Formular y proponer la política y normas para el desarrollo de los sistemas de contabilidad, presupuesto, tesorería y abastecimiento. • Planear, organizar, dirigir, coordinar y controlar la administración de los recursos financieros y materiales. • Ejecución y evaluación periódica del presupuesto de la Universidad de acuerdo a normas y dispositivos vigentes. • Prever a los diferentes órganos conformantes de la Universidad los recursos financieros y materiales que requieran de acuerdo a sus necesidades. • Llevar un control adecuado de los fondos de la Universidad según lo establecido en las normas de sistema de tesorería. • Controlar la ejecución de todos los proyectos productivos de los bienes patrimoniales de la Universidad según las normas establecidas.

UNIDAD ORGANICA	FUNCIONES
<p style="text-align: center;">CONTABILIDAD</p>	<ul style="list-style-type: none"> • Organizar, implementar, controlar y evaluar el sistema de contabilidad de la Universidad. • Elaborar, proponer la normatividad interna para el cumplimiento de funciones y procedimientos de la unidad. • Llevar la contabilidad de la universidad y presentar la información financiera de: Balance General, estado de ganancias y pérdidas, estado de cambio de patrimonio neto, estado de flujos efectivos, registro de activos y pasivos, otros documentos contables. • Ejercer el control previo y concurrente de las operaciones contables y financieras de la Universidad de acuerdo a las normas del sistema de control. • Revisar y verificar la utilización correcta de los bienes económicos, ya sea en el giro de cheques bancarios, pagares, ahorros en moneda nacional, moneda extranjera y

	<p>certificados bancarios en moneda extranjera.</p> <ul style="list-style-type: none">• Revisar, verificar, codificar las rendiciones de cuenta efectuadas en comisión de servicios/gastos efectuados en general.• Registro y elaboración del cálculo de previsión de beneficios sociales.• Asesorar a los diferentes órganos de la Universidad en asuntos de su competencia.• Registro del movimiento contable en los libros principales y auxiliares de contabilidad.• Registrar y analizar las cuentas analíticas (clase 9), y cuentas de gestión (clase 6).• Registrar y analizar las cuentas de resultados (clase 7 y 8).• Registrar en tarjetas el control de cuentas corrientes en adelantos de remuneraciones, entregas a rendir cuenta, anticipo por compra de bienes y servicios, cuentas por pagar, cuentas por cobrar y establecer saldos en forma mensual.
--	---

	<ul style="list-style-type: none"> • Registrar y analizar las cuentas de balance (clase 1, 2, 3, 4, 5). • Registrar y elaborar notas de contabilidad con ajustes, previo análisis de las cuentas. • Mantener ordenada toda documentación contable y el archivo correspondiente. • Revisar y verificar las informaciones mediante asientos contables que remiten las unidades de: Tesorería, abastecimientos, patrimonio y remuneraciones. • Codificar en los comprobantes de pago lo correspondiente a la clase 6, 7, 8 cuentas de resultados. Cuentas analíticas (clase 9) y registros correspondientes: Mediante hojas de trabajo y en forma mensual. Así mismo los ingresos y egresos de caja. • Controlar y verificar los saldos bancarios en forma mensual. • Elaborar y registrar la ejecución presupuestal de ingresos y egresos. • Otras que le asigne el jefe de oficina.
--	--

UNIDAD ORGANICA	FUNCIONES
TESORERÍA	<ul style="list-style-type: none"> • Preparar normas y directivas para la ejecución de las actividades de la unidad. • Recepcionar, registrar, controlar y depositar los fondos por toda fuente de ingreso y egreso a la unidad. • Coordinar las acciones inherentes a la administración de fondos con las oficinas de economía, personal, planificación universitaria y Vice-Rectorado Administrativo. • Mantener el registro en el libro de caja bancos de: Comprobantes de caja, ingresos, egresos. • Giro de cheques por fuente de financiamiento. • Formular las consolidaciones del movimiento de fondo, así como las consolidaciones de subcuentas y cuentas corrientes. • Formular la información para la elaboración de balance mensual.

TESORERIA

- Llevar el registro de control de anticipos.
- Elaboración de comprobantes de pago, así como sus respectivos cheques según fuente de financiamiento.
- Registrar el movimiento diario en le libro bancos.
- Recepción, elaboración, remisión y archivo de correspondencia.
- Manejo de fondo fijo.
- Pago de los servicios por electricidad, agua, teléfono y otros que se le brinda a la Universidad.
- Control de cuentas corrientes de pensiones de enseñanza y otros de alumno regulares. Profesionalización y cursos de complementación.
- Información sobre estado de cuentas de los estudiantes y otros.
- Elaborar resumen por pago de pensiones mensualmente.
- Expedir constancia de no adeudar pensiones y otros a la Universidad.
- Elaborar el resumen de ingresos diarios y

	<p>la información estado mensual ingresos.</p> <ul style="list-style-type: none"> • Organiza y mantiene organizado el archivo. • Emite informaciones relacionadas con el movimiento de ingresos. • Organizar y mantener en orden los recibos de pagos y facilitar la búsqueda de recibos extraviados por los alumnos. • Registrar la salida y entrada de tarjetas de control de pagos de alumnos regulares de Profesionalización y Complementación. • Control del código de matrícula de cada alumno y la verificación correspondiente en los reportes del banco. • Actualización y control de registros de Kardex, para establecer los saldos de los alumnos y ser considerado en el control de kardex general. • Recepción y registro de notas de abono de los bancos y control de los mismos. • Presentar informes periódicos sobre la labor realizada. • Otras que se le asigne y que le corresponda por disposiciones vigentes.
--	---

UNIDAD ORGANICA	FUNCIONES
<p style="text-align: center;">ABASTECIMIENTO</p> <p style="text-align: center;">Y</p> <p style="text-align: center;">PATRIMONIO</p>	<ul style="list-style-type: none"> • Elaborar normas y directivas para el funcionamiento de la unidad. • Conducir al desarrollo de los procesos técnicos de almacenamiento, custodia y distribución de acuerdo a las normas generales del sistema supervisando las labores de personal a su cargo. • Proponer normas y procedimientos de aplicación institucional, en el campo de su competencia. • Proponer el nombramiento de las comisiones de toma de inventarios físicos, bienes de almacén. Así como de activo de la Universidad. • Velar por el mantenimiento, conservación y seguridad de los bienes almacenados. • Preparar las solicitudes de cotizaciones. • Registrar y controlar las solicitudes de cotizaciones y el cuadro comparativo de cotizaciones.

	<ul style="list-style-type: none">• Elaborar las ordenes de compra codificadas debidamente valorizadas.• Programar las compras.• Registrar y controlar las ordenes de compra ingresadas al área de almacén y la correspondiente confrontación con la unidad de tesorería para el pago de proveedores.• Formular y/o tramitar las solicitudes de cotización de bienes materiales y servicios no personales, formular el cuadro comparativo de cotizaciones y el acta de otorgamiento de la buena pro de montos mayores a una UIT, en estrecha coordinación con el jefe de la unidad y el Vice-Rectorado Administrativo para su conformidad.• Recolección y verificación de la calidad, recuento de los materiales adquiridos para su internamiento físico en el área de almacén.
--	---

	<ul style="list-style-type: none">• Elaborar el inventario físico de los bienes existentes en almacén.• Remitir al unidad de contabilidad el parte diario de almacén.• Mantener debidamente actualizado el registro de bienes patrimoniales de la Universidad, coordinando e informando sobre su uso, ubicación, estado de conservación, mantenimiento y su recuperación con los cargos y flujos, así como su depreciación y revaluación.• Conciliar los inventarios físicos valorados con los saldos actualizados en registros o libros con los del balance.• Preparar el catalogo de bienes.• Llevar el registro de adquisiciones de bienes y su respectiva distribución.• Recepcionar los bienes previa conformidad de las características y especificaciones técnicas, así como de su calidad, cantidad para su internamiento y/o distribución.
--	---

	<ul style="list-style-type: none">• Velar por el mantenimiento, conservación y seguridad de los bienes almacenados.• Mantener los registros y kardex de existencia de valores de almacén.• Ubicar los bienes recibidos de acuerdo a la codificación y catalogación adoptados.• Entregar a los usuarios los bienes requeridos, mediante el comprobante de salida de (PECOSA).• Mantener actualizado el estado de existencias.• Otras funciones que le asigne el jefe de unidad.
--	---

UNIDAD ORGANICA	FUNCIONES
PERSONAL	<ul style="list-style-type: none"> • Supervisar el cumplimiento de las funciones, directivas y tareas encomendadas al personal docente y administrativo. • Cumplir y hacer cumplir las disposiciones de carácter técnico administrativo; las resoluciones de rectorado y demás disposiciones que norman el funcionamiento de la Universidad. • Implementar los procesos de selección, nombramiento, contrato, reasignación, reingreso, ascenso, evaluación, promoción y control del personal docente y administrativo de la Universidad. • Administrar la política salarial del personal docente y administrativo, y proponer las escalas remunerativas cuando sea necesario.

UNIDAD ORGANICA	FUNCIONES
REMUNERACIONES	<ul style="list-style-type: none"> • Formulación de las plantillas únicas de pago de haberes del personal docente, administrativo, contratado, obrero permanente y eventuales, y formular la boleta única de pagos mensuales. • Formular normas mensuales, directivas, para implementar políticas de administración salarial, orientadas a optimizar el manejo de remuneraciones. • Elaborar el presupuesto analítico de personal, docente y administrativo. En coordinación con la oficina de planificación universitaria. • Proponer acciones para la implementación de la política de remuneraciones. • Elaborar las liquidaciones de beneficios sociales requeridos por los trabajadores, de acuerdo a los dispositivos legales vigentes.

	<ul style="list-style-type: none">• Elaborar las liquidaciones para el cumplimiento de obligaciones de transferencias de la Universidad al ESSALUD, SPP.• Formular certificado de remuneraciones de quinta categoría.• Informar a la oficina de economía el resumen de descuentos realizados con motivo de las remuneraciones mensuales.• Atender e informar a los trabajadores sobre los pagos y descuentos hechos en la planilla de pagos.• Coordinar con el jefe de personal sobre asuntos inherentes a sus funciones.• Las demás funciones que se le asigne.
--	---

UNIDAD ORGANICA	FUNCIONES
<p style="text-align: center;">ESCALAFÓN</p>	<ul style="list-style-type: none"> • Registrar, archivar, organizar y controlar legajos de personal y escalafón y mantenerlos actualizados. • Formular, proponer normas internas de funcionamiento sobre registros, legajos de personal y escalafón. • Planear, dirigir, evaluar, controlar el cumplimiento de las funciones, objetivos y metas que competen al sistema de personal. • Elaborar y hacer aprobar el rol de vacaciones en las instancias correspondientes. • Formular y proponer la política de capacitación del personal administrativo en coordinación con el jefe de oficina. • Atender y absolver consultas y reclamos del personal y todo aquello que concierne a las acciones propias a su cargo. • Coordinar el financiamiento de la capacitación y perfeccionamiento del personal docente y administrativo. • Otras que le asigne el jefe de la oficina del personal.

UNIDAD ORGANICA	FUNCIONES
<p style="text-align: center;">CONTROL DEL PERSONAL</p>	<ul style="list-style-type: none"> • Evaluar y controlar el cumplimiento de las funciones del personal docente y administrativo, en coordinación con la jefatura de la oficina de personal. • Emitir informe sobre los avances de actividades y tareas de las diferentes unidades y áreas a la jefatura de la oficina de personal. • Planear, coordinar y controlar la asistencia de personal administrativo y docente en el horario y rol que han sido programados. • Informar sobre las inasistencias del personal docente y administrativo elaborando el cuadro de récord de trabajo, de informar escalafón para el computo del rol de vacaciones y a la unidad de remuneraciones para el descuento respectivo.

	<ul style="list-style-type: none">• Formular documentos administrativos de sistema de personal.• Programar, organizar, dirigir, supervisar, evaluar y controlar la prestación de servicios de guardiana en las distintas instalaciones de la universidad, programar turnos para el personal de servicio, incluyendo sábados, domingos y feriados.• Atender y absolver consultas y reclamos del personal en todo aquello que concierne a las funciones propias a su cargo.• Organizar y mantener actualizadas las tarjetas de asistencia diarias de cada uno de los trabajadores.• Otras que le asigne el jefe de la oficina de personal.
--	--

UNIDAD ORGANICA	FUNCIONES
<p style="text-align: center;">MANTENIMIENTO Y PRESTACION DE SERVICIOS</p>	<ul style="list-style-type: none"> • Programar, dirigir, ejecutar, controlar y evaluar el mantenimiento de las diferentes dependencias de la Universidad. • Verificar el estado de conservación y limpieza de los locales de funcionamiento académico y administrativo de la Universidad. • Proponer normas internas de funcionamiento de la unidad de mantenimiento. • Velar por el permanente mantenimiento de los equipos, instalaciones y demás bienes de la Universidad. • Elaborar presupuestos para trabajos específicos de mantenimiento, reparación y verificar su calidad. • Coordinar con el personal técnico la reparación de desperfectos en los servicios

	<p>de agua, desagüe, alumbrado eléctrico, etc., en los ambientes de la universidad.</p> <ul style="list-style-type: none">• Elabora en coordinación con la unidad de control de personal los roles de servicio, turno de los guardianes en los diferentes pabellones académicos y administrativos de la Universidad.• Preparar y presentar informes periódicos de la labor realizada.• Otras que le asigne el jefe de la oficina.
--	---

ENTIDADES ACADÉMICAS:

OBJETIVOS

UNIDAD ORGANICA	OBJETIVOS
VICE RECTORADO ACADEMICO	<ul style="list-style-type: none">• Reemplazar al rector en los casos de vacancia, licencia ausencia o impedimento temporada.• Coordinar las actividades académicas entre las facultades Carreras Académico Profesionales, Institutos, Escuela o secciones de Post-Grado demás unidades Académicas dentro del espíritu de la Ley Universitaria, Estatuto Universitario y el presente Manual.• Presidir las comisiones que estudien y fundamenten la creación, fusión, supresión o reorganización de las unidades académicas que menciona el numeral anterior.• Coordinar y controlar el funcionamiento de las siguientes oficinas: Admisión, Servicios Académicos, Oficina de

	<p>Investigación, Extensión Universitaria y Proyección Social.</p> <ul style="list-style-type: none">• Elevar al Rector los proyectos de Resoluciones que tengan que ver con las actividades académicas.• Coordinar y supervisar con los Decanos de las Facultades la programación, ejecución y evaluación del quehacer académico.• Firmar los certificados de Estudios y las constancias conjuntamente con el jefe de oficina de Servicios Académicos y el Secretario General.• Informar periódica y oportunamente al Rectorado el avance cronológico y académico de la Universidad.• Preparar los documentos para la elaboración de la Memoria del Rector, dentro de su campo.
--	--

UNIDAD ORGANICA	OBJETIVOS
SERVICIOS ACADEMICOS	<ul style="list-style-type: none"> • Lograr la más alta calidad en las tareas académicas de la Universidad, mediante la coordinación y Evaluación del funcionamiento de las facultades. • Centralizar, sistematizar, controlar, fiscalizar y supervisar la información académica. • Prestar servicios de biblioteca, impresión, cómputo.

UNIDAD ORGANICA	OBJETIVOS
<p style="text-align: center;">OFICINA PERMANENTE DE ADMISION</p>	<ul style="list-style-type: none"> • Permitir el ingreso en estricto orden de méritos de estudiantes a las diferentes carreras académicas profesionales de la UANCV, por medio del examen del Admisión, en función a la necesidad de profesionales para la Región y el País.

UNIDAD ORGANICA	OBJETIVOS
<p style="text-align: center;">OFICINA DE INVESTIGACION</p>	<ul style="list-style-type: none"> • Promover la labor de investigación en la Universidad, dentro de los límites fijados por los principios y objetivos de la UANCV. • Estimular la formación de investigadores. • Difundir los resultados de la investigación científica tecnológica que realiza la UANCV.

UNIDAD ORGANICA	OBJETIVOS
<p>CENTRO PRE UNIVERSITARIO</p>	<ul style="list-style-type: none"> • Brindar los servicios educacionales, actualización y afianzamiento de conocimientos y habilidad a los estudiantes egresados de educación secundaria que participen en el CPU. • Promover, promocionar dentro del ámbito educacional de los colegios secundarios sobre la importancia y rol que desempeña la Carrera Universitaria en el desarrollo de nuestra región y de nuestro país.

UNIDAD ORGANICA	OBJETIVOS
<p data-bbox="254 904 636 1092" style="text-align: center;">OFICINA DE EXTENSION UNIVERSITARIA Y PROYECCION SOCIAL</p>	<ul style="list-style-type: none"> <li data-bbox="753 526 1343 707">• Conducir los procesos de políticas de Proyección social de la Universidad a la comunidad. <li data-bbox="753 832 1343 1013">• Conducir y dirigir la cultura y el arte como proyección social y extensión hacia la comunidad. <li data-bbox="753 1137 1343 1559">• Promoción y difusión de la Educación y la Cultura, la investigación y la prestación de servicios profesionales, para generar los cambios culturales y tecnológicos para el desarrollo, económico y social de Juliaca y la Región.

ENTIDADES ACADEMICAS:

FUNCIONES

UNIDAD ORGANICA	FUNCIONES
VICE RECTORADO ACADEMICO	<ul style="list-style-type: none">• Reemplazar al Rector en caso de vacancia, licencia ausencia o impedimento temporada.• Coordinar las actividades académicas entre las facultades carrera académico profesionales, Institutos, Escuela o secciones de Post-grado.• Presidir las comisiones que estudien y fundamenten la creación, fusión, supresión o reorganización de las unidades Académicas.• Coordinar y controlar el funcionamiento de las siguientes oficinas: Admisión, Servicios Académicos, Investigación y Bienestar Universitario y Proyección Social.

	<ul style="list-style-type: none">• Eleva al rector los proyectos de Resoluciones que tengan que ver con las actividades académicas, tales como la aprobación de la curricula, los traslados internos y externos, las reservaciones de matrícula y otros.• Coordina y supervisa con los Decanos de las Facultades la programación, ejecución del quehacer académico.• Firma los certificados de estudios y las constancias, conjuntamente con el Jefe de Oficina de servicios Académicos y el Secretario General.• Informa periódica y oportunamente al rectorado el avance cronológico y académico de la Universidad.• Prepara los documentos para la elaboración de la Memoria del Rector, dentro de su campo.
--	--

UNIDAD ORGANICA	FUNCIONES
<p>SERVICIOS ACADEMICOS</p>	<ul style="list-style-type: none"> - Planifica, programa, organiza, dirige y evalúa el desarrollo académico. - Formular la normatividad interna de las acciones académicas de las Facultades. - Propone planes de acción para el eficaz funcionamiento de las facultades.

UNIDAD ORGANICA	FUNCIONES
<p style="text-align: center;">OFICINA PERMANENTE DE ADMISION</p>	<ul style="list-style-type: none"> • Coordinar con las facultades de la Universidad el establecimiento de vacantes, el mismo que deberá ser ratificado por consejo universitario. • Formular y aprobar el reglamento de concurso de Admisión correspondiente al semestre en el cual se lleva el proceso y elevarlo a consejo universitario para su aprobación. • Dirigir, coordinar, ejecutar y evaluar la realización de los procesos de concurso de Admisión. • Dar cuenta al consejo universitario sobre los resultados de proceso del concurso de Admisión. • Dar cuenta al consejo Universitario sobre los resultados del proceso del concurso de Admisión. • Elaborar un banco de preguntas para los exámenes de admisión. • Elaborar un banco de preguntas para los

	<p>exámenes de admisión.</p> <ul style="list-style-type: none"> • Asegurar el cumplimiento de los objetivos de la Comisión de Admisión. • Coordinar con las Facultades de la Universidad el establecimiento de vacantes, el mismo que deberá ser ratificado por Consejo Universitario. • Formular el Reglamento de concurso de Admisión correspondiente al semestre en el cual se lleva el proceso. • Coordinar la fecha de Inicio del ciclo pre-universitario y el reglamento de evaluaciones del ciclo, con el Coordinador del Centro Pre-Universitario. • Dirigir la programación, inscripción, evaluación y publicación de resultados del examen de admisión. • Remitir los resultados del examen de admisión y de todo lo actuado al Consejo Universitario en un plazo máximo de 20 días.
--	--

	<ul style="list-style-type: none">• Establecer un archivo de la documentación del Proceso de Admisión, asimismo de los bienes y enseres de la Oficina.• Formular el presupuesto de la oficina permanente de Admisión y remitirlo a la oficina de Planificación Universitaria.• Remitir a Consejo Universitario los resultados de ingresantes a la Universidad del Centro Pre-Universitario para la emisión de la resolución correspondiente.• Resolver cualquier caso no contemplado en el Reglamento de Examen de Admisión.• Remitir el Reglamento del Centro Pre-Universitario al Consejo Universitario para su aprobación.• Aprobar el presupuesto de ingresos y egresos del centro Pre-Universitario.
--	--

UNIDAD ORGANICA	FUNCIONES
<p style="text-align: center;">OFICINA DE INVESTIGACION</p>	<ul style="list-style-type: none"> • Proponer políticas y estrategias de investigación y asegurar su cumplimiento. • Aprobar y autorizar los proyectos de investigación de las propuestas por las comisiones de investigación de las facultades o por los docentes a iniciativa propia. • Mantener una relación permanente con entidades Públicas o Privadas para lograr los objetivos de investigación de la UANCV. • Identificar y proponer a Consejo Universitario, la captación de recursos de cooperación técnica nacional e internacional y afiliarse a organismos nacionales e internacionales.

UNIDAD ORGANICA	FUNCIONES
<p style="text-align: center;">CENTRO PRE UNIVERSITARIO</p>	<ul style="list-style-type: none"> • El coordinador del Centro Pre-Universitario, es el encargado de asegurar el cumplimiento de las políticas y normas establecidas por el Reglamento del Centro Pre-Universitario. • Ejercer la representación legal del centro Pre-Universitario. • Participar como miembro activo en la comisión de admisión de la universidad Andina "Nestor Cáceres Velásquez". • Dirigir, coordinar y supervisar las acciones educativas del centro Pre-Universitario. • Preparar el presupuesto de ingresos y egresos, los planes de trabajo, la memoria y los balances para su presentación al Consejo Universitario.

	<ul style="list-style-type: none">• Nombrar las comisiones que estime necesarias para el cumplimiento del objetivo del centro pre-universitario.• Ejecutar el presupuesto aprobado del centro Pre-Universitario dentro de los márgenes permisibles.• Ejecutar las acciones de la administración y de personal.• Fomentar la organización, participación o coordinación de seminarios o conferencias, visitas relacionadas con la carrera académica profesionales con que cuenta la UANCV.• Mantener intercambio de información con entidades similares nacionales y/o extranjeras.• Emitir los informes y/o proporcionar la información que le fuere solicitada por las autoridades universitarias y/o educativas.
--	---

	<ul style="list-style-type: none">• Revisar y estudiar los asuntos a ser coordinados con el presidente de la comisión de administración.• Preparación de la información contable en base a los estado y análisis financieros y ejecución presupuestal a ser presentados al Vice Rectorado administrativo.• Presentar informes a Vice Rectorado administrativo para los pagos del personal docente y administrativo, en base a las normas legales vigentes.• Otras inherentes a su cargo.
--	---

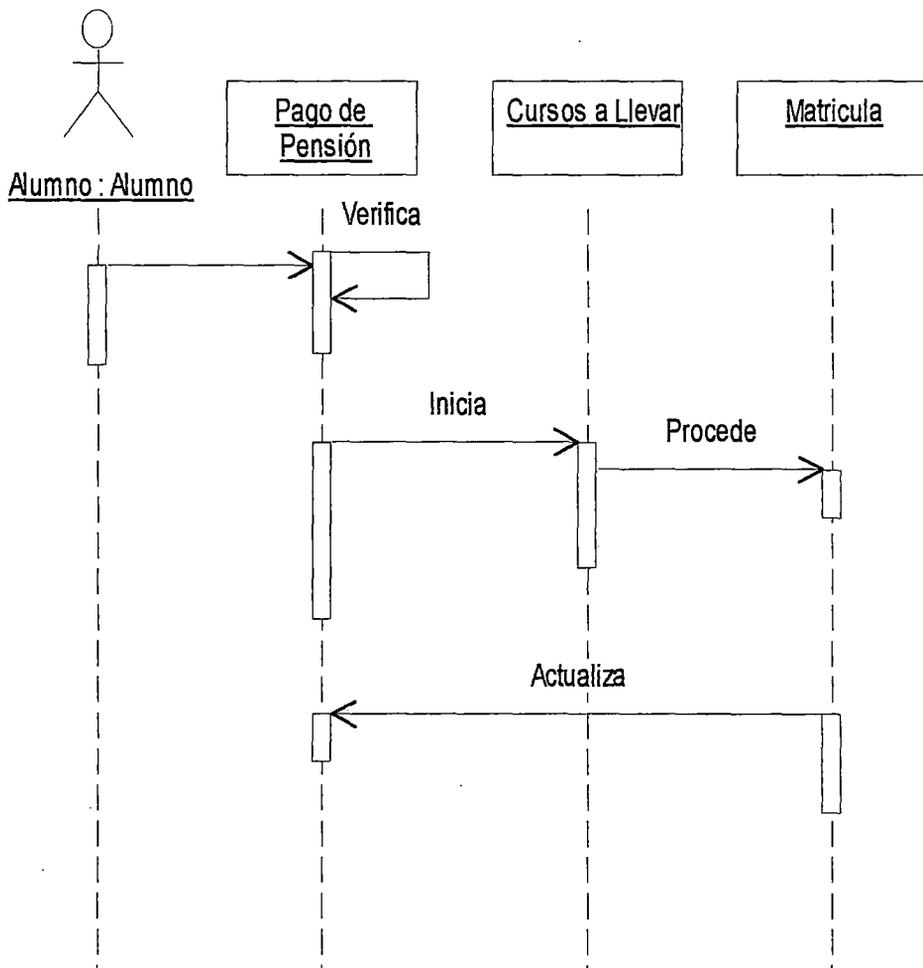
UNIDAD ORGANICA	FUNCIONES
<p style="text-align: center;">OFICINA DE EXTENSION UNIVERSITARIA Y PROYECCION SOCIAL</p>	<ul style="list-style-type: none"> • Promueve actividades académicas y culturales que redunden en beneficio de la población dentro de la cual está inscrita. • Desarrolla acciones sociales a través de la presentación de servicios profesionales, dirigidos posteriormente a los sectores económicos sociales más deprimidos. • Promueve los cambios tecnológicos y culturales que beneficien a la población que está bajo el área de influencia de la Universidad; posibilitando de esta manera el impulso del desarrollo nacional y regional.

ANEXO N° 03

DESCRIPCION DEL SISTEMA DE INFORMACIÓN

ADMINISTRATIVO DE LA U.A.N.C.V

DIAGRAMA DE SECUENCIA DE LA MATRICULA



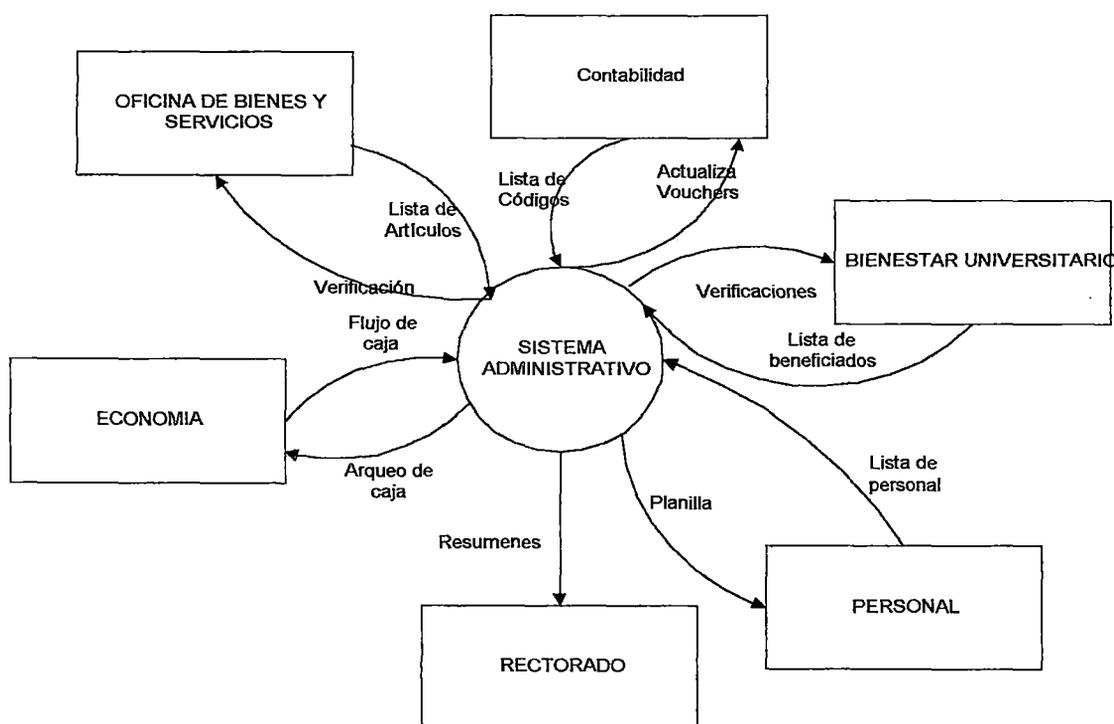
A. DESCRIPCION DEL SISTEMA DE GESTION ADMINISTRATIVA

Se encarga de la administración de los sistemas de información relacionados con la logística, planillas, Presupuesto, tesorería, contabilidad y abastecimientos de la Universidad, con la finalidad de satisfacer los requerimientos de cada entidad de la Universidad. Para el análisis y diseño orientado a objetos empezaremos por cada módulo para así luego del ensamblaje formar un todo.

DIAGRAMA DE CONTEXTO

En la Figura 1. Mostramos el diagrama de contexto del Sistema de Gestión Administrativo, observamos que las entidades que interactúan con dicho sistema son:

FIGURA 1



1. SISTEMA DE LA UNIDAD DE ABASTECIMIENTO Y PATRIMONIO

El ciclo de datos de todo sistema de logística, comienza con una requisición de compra de materiales o equipos, determinada por los requerimientos operativos de la entidad, continúa con la emisión de una orden de compra, la posterior recepción del material o el equipo ordenado, y concluye con la conversión de dinero de caja en un gasto o un activo. (Figura 3)

Responsabilidades:

- 1.- Generación de requisiciones.
- 2.- Control Presupuestal.
- 3.- Determinación de la cantidad a comprar.
- 4.- Selección del proveedor.
- 5.- Emisión de órdenes de compra.
- 6.- Recepción de Materiales.
- 7.- Registro de cuentas por pagar.
- 8.- Pagos a Proveedores.
- 9.- Registro de los asientos contables correspondientes.

Generación de Requisiciones

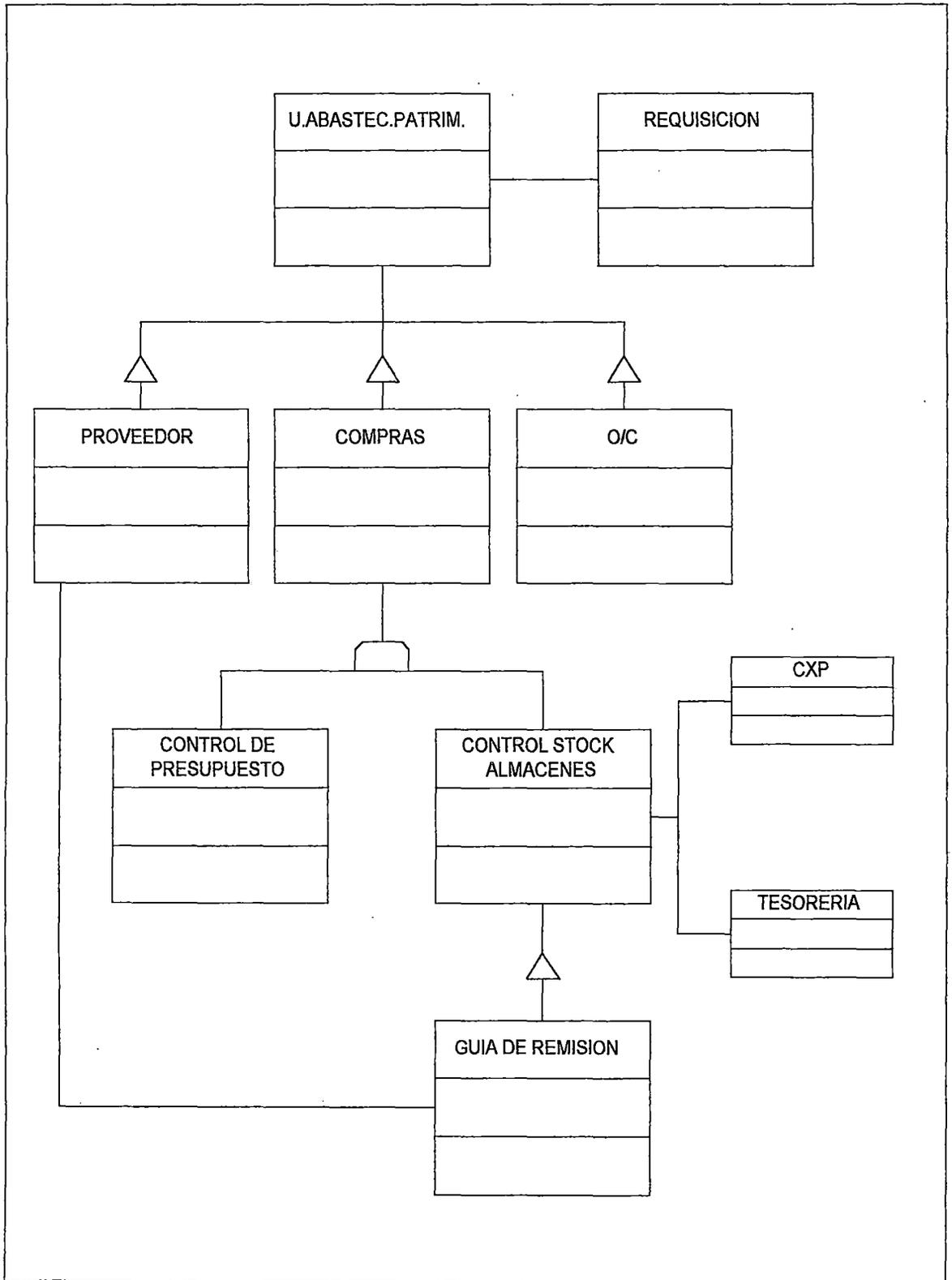
Cuando por requerimientos operativos o por la necesidad de mantener los niveles mínimos de inventarios para el suministro de insumos o repuestos, los departamentos responsables emiten requisiciones de compra, indicando por lo menos la siguiente información para cada Item:

Objeto : Requisición

Atributos:

Cod_Req	C(8)	* Código de la requisición
Descripcion	C(60)	* Descripción del Item
Cantidad	N(8)	* Cantidad requerida
Plazo_Ent	D(8)	* Plazo de entrega requerido
Fecha_Emis	D(8)	* Fecha de Emisión
Partida	N(15,2)	* Partida presupuestal que afectará la adquisición

OBJETO DE ABASTECIMIENTO Y PATRIMONIO



1.1. Control Presupuestal

El Dpto de Compras efectúa la verificación de la existencia de saldo en la partida presupuestal correspondiente, y eventualmente su afectación o compromiso, para evitar que otras requisiciones en curso puedan originar su sobregiro.

1.2. Determinación de la cantidad a Comprar

El Dpto. de Compras determina la cantidad a comprar en función a diferentes criterios, tales como el mantenimiento de stocks mínimos, o la determinación de “Lotes Económicos de Compra”, y eventualmente por restricciones de cantidades mínimas de despacho de los proveedores. También es importante la consolidación de requisiciones procedentes de diversas áreas de la entidad, que pueden requerir los mismos equipos o materiales.

1.3. Selección de Proveedor

De acuerdo al R.U.A. se procederá a la selección del proveedor ya sea por concurso de precios o licitación pública, según el monto total de la compra o del tipo de bienes que se va a adquirir.

1.4. Emisión de órdenes de compra

Las órdenes de compra emitidas y remitidas a los proveedores están a disponibilidad (Por medio electrónico o mediante copia física) de los puntos de recepción o almacenes, y de las áreas de contabilidad, tesorería y de las áreas que efectuaron las requisiciones pertinentes.

También cabe resaltar que el sistema cuenta con un reporte o pantalla de seguimiento de las ordenes de compra emitidas y pendientes de atención por los proveedores.

Objeto : Orden

Atributos:

Cabecera

Num_oc	C(8)	* N° de Orden de Compra
Des_Prov	C(60)	* Identificación y dirección del proveedor
Fech_Emision	D(8)	* Fecha de Emisión
Plazo_Ent	D(8)	* Plazo de Entrega
Lugar	C(40)	* Lugar de Entrega
Condición	C(1)	* Condiciones de pago (Contado, crédito,..)

Detalle (Por cada item)

Descripción	C(80)	* Descripción de material o equipo ordenado
Cantidad	N(8)	* Cantidad Ordenada
Unidad	C(5)	* Unidad de medida
Precio	N(8,2)	* Precio Unitario
Descuentos	N(8,2)	* Descuentos
Total	N(8,2)	* Total por Item

Recepción de Materiales

Los almacenes o puntos de recepción de los materiales o equipos ordenados registran en el sistema el ingreso a conformidad de los materiales o equipos ordenados registrarán en el sistema el ingreso a conformidad de los materiales o equipos recibidos, indicando cantidad y fecha de recepción por cada ítem, así como el proveedor y N° de Orden de Compra que originó la entrega.

Registro de cuentas por pagar

Una vez recepcionado el material se registran las cuentas por pagar correspondientes, en función de las cantidades recibidas, las condiciones de precio y condiciones de pago especificadas en la orden de compra.

Pagos a Proveedores

El área de Tesorería podrá efectuar los pagos a proveedores contra las facturas que presenten, para lo cual el sistema debe llevar un control sobre las cuentas por pagar pendientes, y comprobar si las facturas corresponden a las ordenes de compra respectivas, y si los bienes ordenados han sido recibidos a conformidad, registrando los egresos de caja correspondientes.

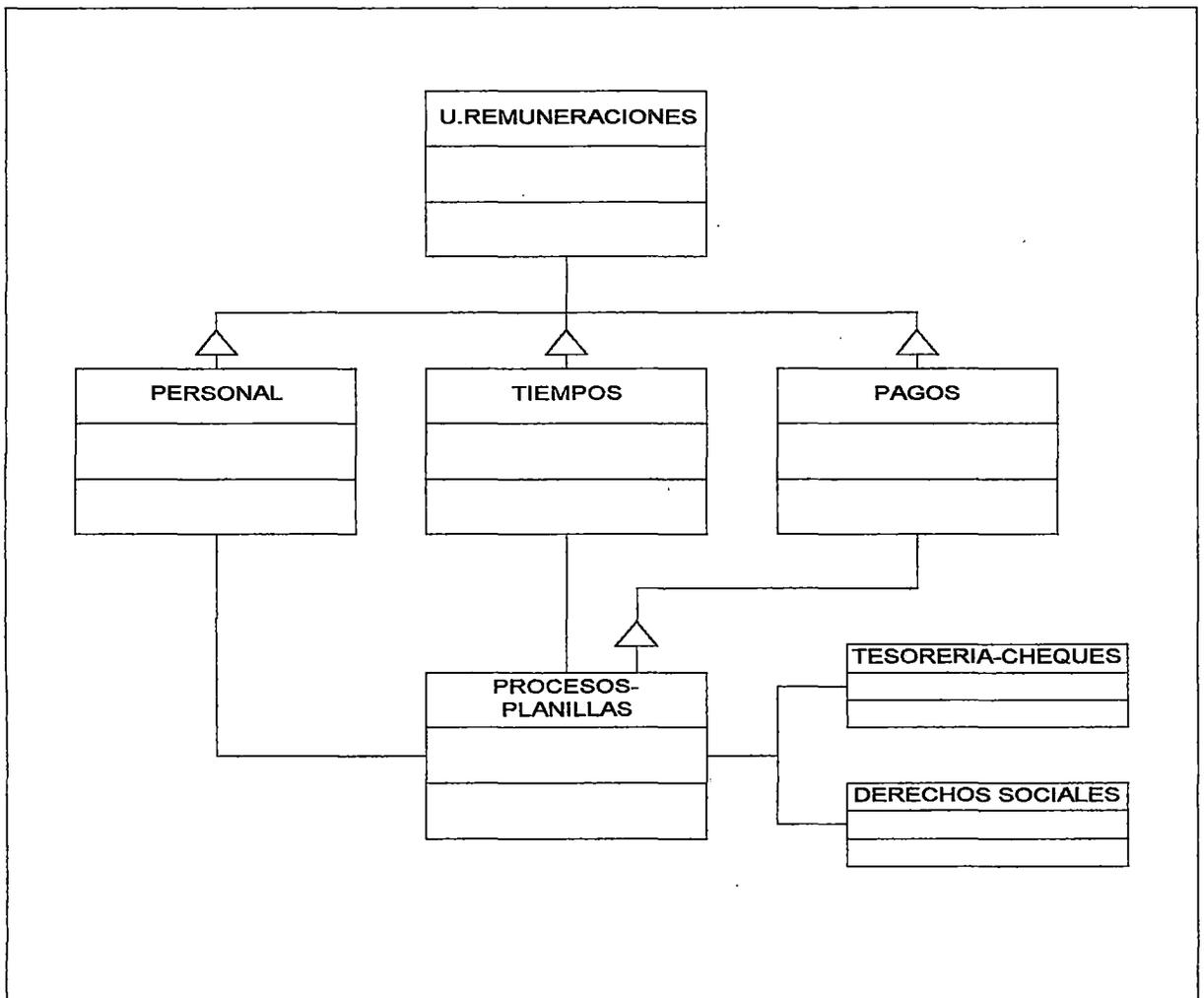
Registro de los asientos contables correspondientes

El ciclo del sistema logístico sólo estará completo, si se ha efectuado el registro de los asientos contables que se deben generar cuando se producen los eventos respectivos.

2. Sistema de la Unidad de Remuneraciones

El ciclo de datos de los sistemas de planillas de la Unidad de Remuneraciones es relativamente simple, comienza con la actualización de los datos básicos de cada servidor, la recolección de la información de tiempos laborados y la actualización de datos externos, tales como tasas de impuestos, cotizaciones y otros. (Figura 4)

OBJETO - REMUNERACIONES



Con esta información al día de cierre, el sistema de planillas procesa y emite la planilla de pago de los servidores de la entidad. Este Sistema, constituye un sistema de misión crítica, ya que cualquier inconveniente, error o atraso en su emisión, afectará el pago de los sueldos de los servidores, y puede generar problemas serios en el funcionamiento y operatividad de la entidad.

Responsabilidades:

- 1.- Mantenimiento de la información básica de cada servidor.
- 2.- Registro y control de tiempos laborados.
- 3.- Rol y control de uso de vacaciones.
- 4.- Cálculo de conceptos de pago y deducciones.
- 5.- Control presupuestal.
- 6.- Emisión de la Planilla de Pago.
- 7.- Emisión de Cheques de Pago.
- 8.- Registro de los asientos contables correspondientes.

2.1. Mantenimiento de la Información básica de cada servidor

Esta información esta de acuerdo a los Cuadros de Asignación de Personal correspondiente a cada uno de los Dptos respectivos, y se debe actualizar, crea nuevos registros cuando ingresa nuevo personal, con el retiro de algún servidor por renuncia o despido, o cuando se producen variaciones en los ingresos o en las deducciones de cada servidor.

La actualización de esta información debe estar respaldada por documentos que estén refrendados por las autorizaciones pertinentes.

Objeto: Pagos

Atributos:

Nombres	C(40)	* Apellidos y nombres del servidor
Area	C(20)	* Area o Dpto. donde trabaja
Cargo	C(10)	* Cargo que ocupa
Fecha-ini	D(8)	* Fecha de ingreso a la entidad
Fecha-fin	D(8)	* Fecha de salida de la entidad
Categoría	C(10)	* Homologación o categoría
Sueldo_Basico	N(15,2)	* Sueldo Básico
Bonificación	N(10,2)	* Bonificación al cargo
Otros_Pagos	N(10,2)	* Otros pagos
Deducciones	N(10,2)	* Deducciones de Ley
Deducc_Jud	N(10,2)	* Deducciones Judiciales
Otras_Deducc	N(10,2)	* Otras deducciones
Saldo	N(15,2)	* Saldo Neto a Pagar

2.2. Registro y control de tiempos laborados

El Origen de la información de tiempos de ingreso y salida diaria del centro de trabajo, es manual mediante tarjetas marcadas por relojes. El registro de la información debe cerrarse diariamente y deben emitirse reportes diarios y resúmenes mensuales del tiempo laborado por cada trabajador.

2.3. Rol y Control de uso de vacaciones

Es por medio manuales la cual mantiene un Rol de vacaciones y control del uso efectivo para todos los trabajadores.

2.4. Cálculo de conceptos de pago y deducciones

El proceso de cálculo de los pagos totales a los que tiene derecho cada trabajador incluirá su sueldo básico, la remuneración al cargo, y los ingresos por bonificaciones especiales (Escolaridad, Fiestas Patrias, etc.).

El proceso de cálculo de las deducciones incluirá las deducciones por tardanzas y horas no laboradas de acuerdo al registro y control de tiempo laborado, las deducciones de ley (FONAVI, ESSALUD, AFP, CTS, Impuesto de Quinta categoría etc.), las deducciones judiciales si las hubiere, y cualquier otra deducción debidamente autorizada (Ej: Prestamos administrativos, etc.). Y con los pagos y deducciones se calcula el saldo neto a pagar.

2.5. Control Presupuestal

En función de los montos calculados el sistema debe verificar la existencia de saldos positivos en las cuentas presupuestales correspondientes a cada uno de los Dptos a los que pertenecen los servidores, así como también debe generar la afectación de cuentas del presupuesto de gastos de la entidad.

2.6. Emisión de la Planilla de Pago

Una vez efectuado el control presupuestal el sistema emite la Planilla de Pagos para su remisión al Ministerio de Trabajo y emite simultáneamente las boletas de Pago con la misma información para su entrega a los trabajadores, las que deben tener cargo de recepción firmado por cada uno de los trabajadores, como constancia del pago recibido.

2.7. Emisión de Cheques de Pago

La emisión automática de Cheques de Pago debe ser autorizado y supervisado por el responsable directo de la emisión de la planilla y por el tesorero, debiéndose llevar un registro de los cheques emitidos y anulados para asegurar el cumplimiento propio de dichos pagos y de su posterior conciliación bancaria.

2.8. Registro de los asientos contables correspondientes

El Sistema de planillas debe generar los asientos contables correspondientes a los pagos y retenciones que efectúa la entidad, por cuenta propia y de terceros, tales como:

- Pago de remuneraciones.
- Cuentas por pagar por retenciones.
- Provisiones para beneficios sociales.
- Deudas del personal.
- Gastos de Personal.
- Transferencias por prestaciones sociales.

- Impuesto a las remuneraciones.
- Provisiones por CTS.

Las cuentas por pagar deben incluir todos los compromisos de pago que afecten las cuentas del presupuesto de la entidad que se audita, tales como, cuentas por pagar a proveedores, remuneraciones y pensiones y otras.

2.9. Tesorería

La aplicación de Tesorería permite un control estricto del efectivo, la administración y la emisión de cheques, para lo cual debe de poseer mecanismos de registro y control de pagos, los que simultáneamente a su ejecución, deben de generar y registrar los asientos contables correspondientes.

La información que se registre para cada pago debe de incluir, además del voucher correspondiente, la identificación del funcionario que autorizo el pago, la fecha y hora en que se emitió el cheque o se efectuó el pago respectivo, lo cual debe de estar de acuerdo al reglamento de poderes y autorizaciones y al Manual de Procedimientos Contables de la entidad.

2.10. Conciliación Bancaria

La administración de las cuentas corrientes de la entidad y la emisión de cheques por cualquier concepto, sólo se completa con la comprobación de pagos y conciliación de saldos de las cuentas corrientes respectivas, para lo cual ésta

aplicación debe haberse hecho en coordinación con los bancos, los cuales proporcionarán la información de movimiento de las cuentas corrientes de la entidad.

2.11. Contabilidad Presupuestal

Todo el proceso de ejecución presupuestal, debe de ser registrado a través de la contabilidad presupuestal, debiendo registrarse las autorizaciones de giro o desembolsos del tesoro Público que habilitan las partidas de la entidad, así como las transacciones que comprometen las partidas y las transacciones que afectan dichas partidas.

3. SISTEMA DE PRESUPUESTO Y TESORERIA

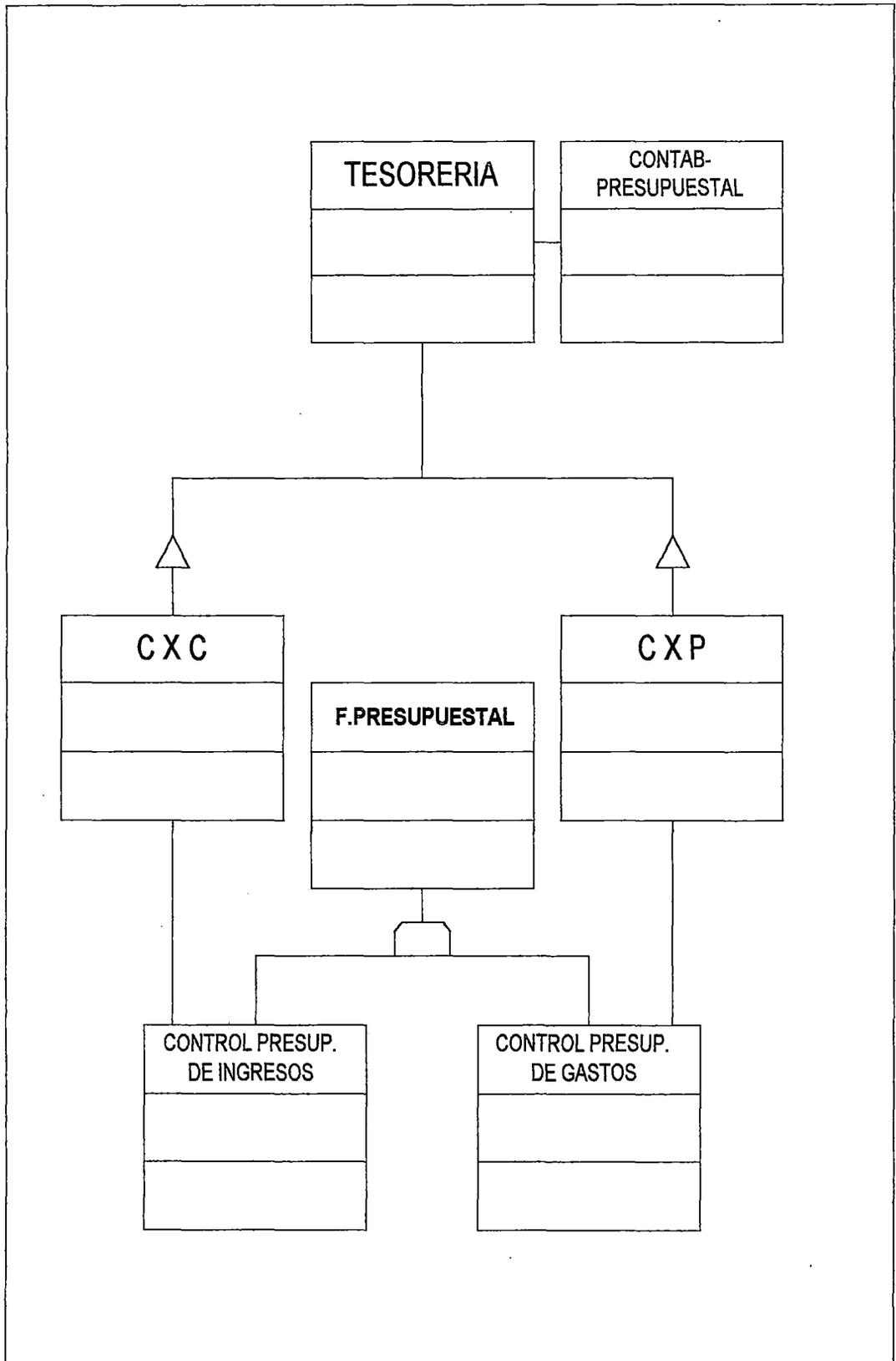
El Ciclo de Información del sistema se inicia con la formulación del Presupuesto, su aprobación por el consejo universitario y su posterior ejecución a lo largo del año.

(Figura 5)

Responsabilidades:

- 1.- Formulación Presupuestal.
- 2.- Control de Presupuesto de Ingresos y Cuentas por Cobrar.
- 3.- Cuentas por Pagar.
- 4.- Control Presupuestal.
- 5.- Tesorería.
- 6.- Conciliación Bancaria.
- 7.- Contabilidad Presupuestal.

OBJETO - TESORERIA



3.1. Formulación Presupuestal

El primer módulo del sistema debe permitir la formulación del presupuesto anual de ingresos y gastos de la empresa, asignando los gastos e inversiones que requiera cada una de las áreas o Dptos de la misma, calendarizando la utilización de las cuentas, mes a mes, en función de las necesidades propias de la gestión y emitiendo los reportes consolidados anuales respectivos.

3.2. Control de Presupuesto de Ingresos y Cuentas por Cobrar

El Presupuesto de ingresos se ejecuta a través del control de ingresos por matriculas, de los ingresos financieros y otras cuentas por cobrar, por lo que es de primera importancia para la marcha eficiente de la empresa, ya que, si no dispone de liquidez, deberá recurrir a la contratación de créditos bancarios, con el consiguiente incremento de costos.

Luego, durante e periodo de ejecución presupuestal, la habilitación de las partidas de gastos correspondientes se efectuará en función de la consecución de los ingresos provenientes de matriculas y/o por el accionar de las carreras que hagan efectiva las Cobranzas.

3.3. Control Presupuestal

Todo sistema de presupuesto dispone de una aplicación de control de la ejecución del presupuesto, mediante la cual todo pago, sea de gasto o inversión, antes de ser ejecutado, debe ser autorizado a través de un proceso de control, que permita

verificar la existencia de saldos positivos en la cuenta presupuestal respectiva, comprometiendo los montos y cuentas correspondientes.

3.4. Cuentas por Pagar

Las cuentas por pagar forman parte de todo sistema de tesorería, y debe de integrarse al sistema de presupuesto como el mecanismo mas seguro de comprometer las cuentas y montos por pagar como compromisos de pago de la empresa.

Las cuentas por pagar deben incluir todos los compromisos de pago que afecten las cuentas del presupuesto de la universidad, tales como, cuentas por pagar a proveedores, remuneraciones y participaciones, tributos, y cuentas por pagar diversas.

3.5. Tesorería

La aplicación de Tesorería debe permitir un control estricto del efectivo, la administración y emisión de cheques, para lo cual debe de poseer mecanismos de registro y control de pagos, los que simultáneamente a su ejecución, deben de generar y registrar los asientos contables correspondientes.

La información que se registre para cada pago debe de incluir, además del voucher correspondiente, la identificación del funcionario que autorizó el pago, la fecha y hora en que se emitió el cheque o se efectuó el pago respectivo, lo cual debe de estar de acuerdo al Reglamento de Poderes y Autorizaciones y al Manual de Procedimientos Contables de la entidad.

Siendo el efectivo el recurso mas crítico de la empresa, su administración debe ser ágil y eficiente, pero a la vez segura, por lo que el sistema debe de proveer todas las facilidades para su eficaz administración, emitiendo reportes diarios de ingresos y pagos, así como de reportes de situación de la disponibilidad de liquidez en cualquier momento.

Adicionalmente la aplicación de Tesorería permite la previsión y planificación del flujo de efectivo, en función de las necesidades y compromisos de pago asumidos, y de la programación de ingresos derivados del control de ventas y cuentas por cobrar.

3.6. Conciliación Bancaria

La administración de las cuentas corrientes de la Empresa y la emisión de cheques por cualquier concepto, sólo se completa con la comprobación de pagos y conciliación de saldos de las cuentas corrientes respectivas, para lo cual ésta aplicación debe haberse hecho en coordinación con los bancos, los cuales proporcionarán la información de movimiento de las cuentas corrientes de la empresa.

3.7. Contabilidad Presupuestal

Todo el proceso de ejecución presupuestal, debe de ser registrado a través de la contabilidad presupuestal, debiendo registrarse los ingresos por Ventas y otros, así como las transacciones que comprometen las partidas y las transacciones que afectan dichas partidas.

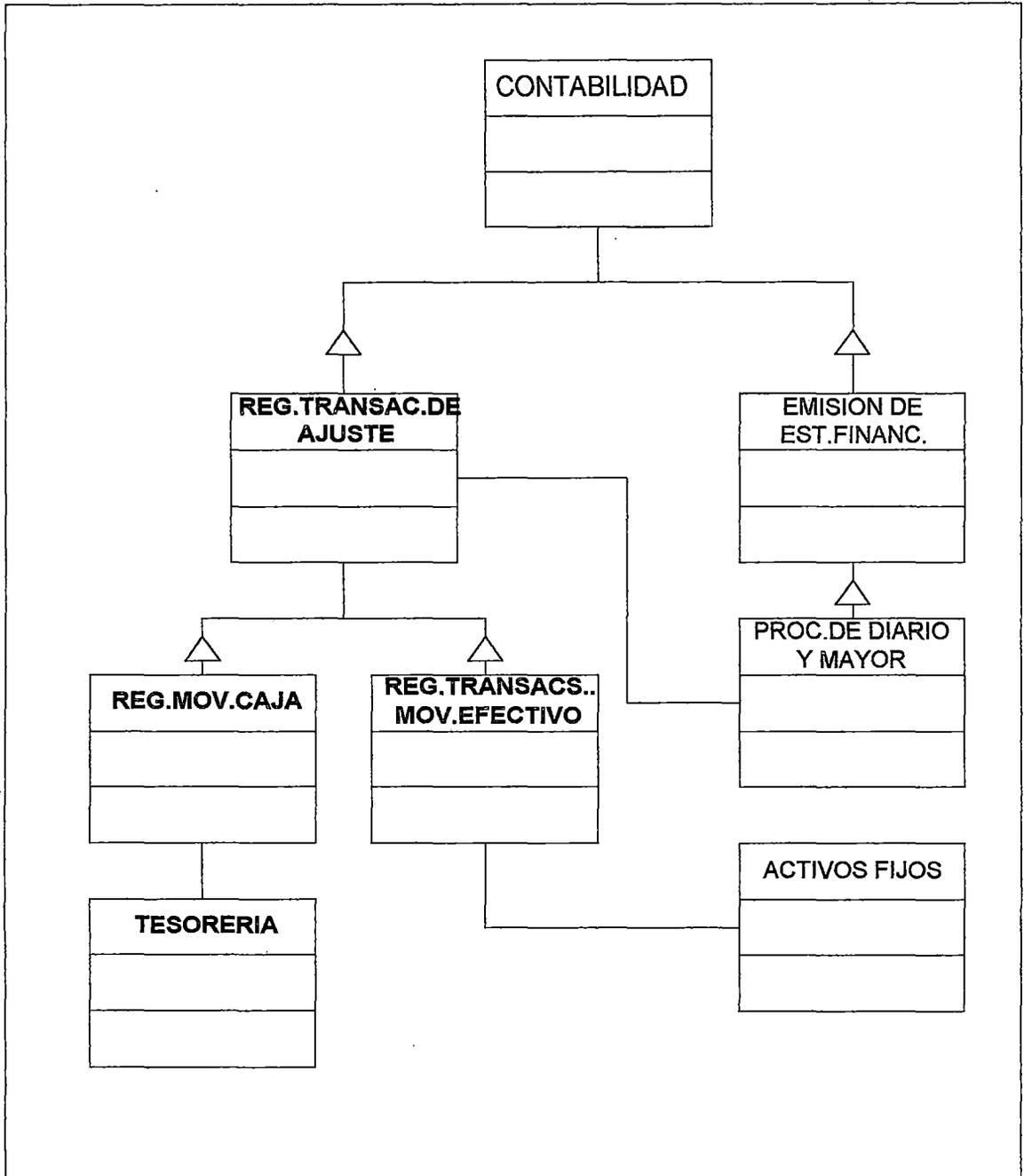
4. SISTEMA DE CONTABILIDAD

El ciclo de información del sistema de contabilidad, se inicia con la generación de transacciones contables, mediante voucher u operaciones que generan asientos contables en los diferentes sistemas de apoyo a la gestión de la entidad, los que al ser registrados, afectan directamente los saldos de las cuentas respectivas, de acuerdo al plan contable, y su proceso al cierre mensual o anual, permite la emisión del Balance y del Estado de Resultados de la entidad. (Figura 6)

Responsabilidades:

- 1.- Registro de movimiento de Caja.
- 2.- Registro de transacciones sin movimiento de efectivo.
- 3.- Registro de transacciones de ajuste.
- 4.- Proceso de Diario y Mayor.
- 5.- Emisión de Balance y Estado de Resultados.

OBJETO - CONTABILIDAD



4.1. Registro de Movimiento de Caja

El registro de movimientos de caja, forma parte del sistema de tesorería y simultáneamente es también parte del sistema de Contabilidad, siendo así, una aplicación de integración de los sistemas de información de la entidad.

Toda transacción contable comprende el movimiento simultáneo de cuentas de débito y de las respectivas cuentas de crédito debidamente balanceadas. El registro de una operación en la cual los débitos no corresponden con exactitud a los créditos denota que existe un error.

Es importante hacer notar, que tomando en conjunto todas las cuentas, la suma de los saldos deudores, debe igualar a la suma de los saldos acreedores, y de no resultar así, es señal de que existe error en el registro de alguna transacción.

4.2. Registro de transacciones sin movimiento de efectivo

Existen muchas transacciones contables que no involucran movimiento de efectivo, tales como la de los ingresos de bienes al almacén, o la provisión para beneficios sociales, etc. Las que son generadas por otros sistemas, o por el contador de la entidad, y todas deben ser registradas de acuerdo a la mecánica siguiente:

- a. Los incrementos de activos son débitos, las disminuciones son créditos.
- b. Los incrementos en capital son créditos, las disminuciones son débitos.
- c. Los incrementos en gastos son débitos, las disminuciones créditos.
- d. Los aumentos en bienes producidos son créditos, las disminuciones son débitos.

4.3. Registro de transacciones de ajuste

El contador de la entidad registrará las transacciones de ajuste para aquellas cuentas que sufren afectaciones que no se evidencien por medio de documentos, tales como las llamadas “transacciones continuas” por el consumo de materiales a granel como los combustibles, las primas de seguros pagadas por anticipado, devengados y otros, así como, el registro de depreciación y revaluación de activos, estos activos se programan y se ejecutan como “asientos automáticos”.

4.4. Proceso de Diario y Mayor

Al cierre del periodo contable, se procesan las transacciones a nivel de cuentas de Diario, como archivo de registro cronológico de las operaciones, para re-clasificarlas, resumirlas o consolidarlas en las cuentas del Mayor.

El archivo de Mayor debe contener, por lo menos, tantas cuentas como partidas figuran en el Balance General y en el Estado de Resultados.

En todos los procesos de cierre, las cuentas de productos y las cuentas de gastos se cierran contra las cuentas de resultados, en las cuales se refleja el superávit o el déficit del periodo contable, mostrando por separado todos los elementos de déficit o superávit, de acuerdo al Plan Contable Gubernamental, efectuando a continuación, el cierre de todas las cuentas para el período contable en cuestión con el asiento de Diario respectivo, los que se pasan al Mayor para determinar los asientos de reversión, si fuesen necesarios.

4.5. Emisión de Balance y Estado de Resultados

La emisión del Estado de Resultados y del Balance, es el producto final del proceso del Diario y Mayor, el cual eventualmente puede presentar errores, para lo cual un Auditor de Sistemas puede pedir ayuda al Dpto. de Cómputo.

5. SISTEMA DE ACTIVO FIJO

El ciclo de información se inicia con el registro en “libros” del sistema de contabilidad de un activo fijo, su asignación a la unidad operativa que va a usarlo, que va a ser responsable de su cuidado y de su conservación; y por último, la realización de inventarios periódicos, hasta su eventual baja. (Figura 7)

Responsabilidades:

- 1.- Registro y actualización de Activos Fijos (Altas y Bajas).
- 2.- Asignación de Activos Fijos.
- 3.- Inventarios de Activos Fijos.

5.1. Registro y actualización de Activos Fijos (Altas y Bajas)

El proceso de registro de un activo en el archivo de Activos Fijos, es decir su Alta, es una operación simultánea con su registro como operación contable, y contablemente su alta se registra a su valor de Costo (Costo instalado y listo para funcionar).

OBJETO - ACTIVOS FIJOS

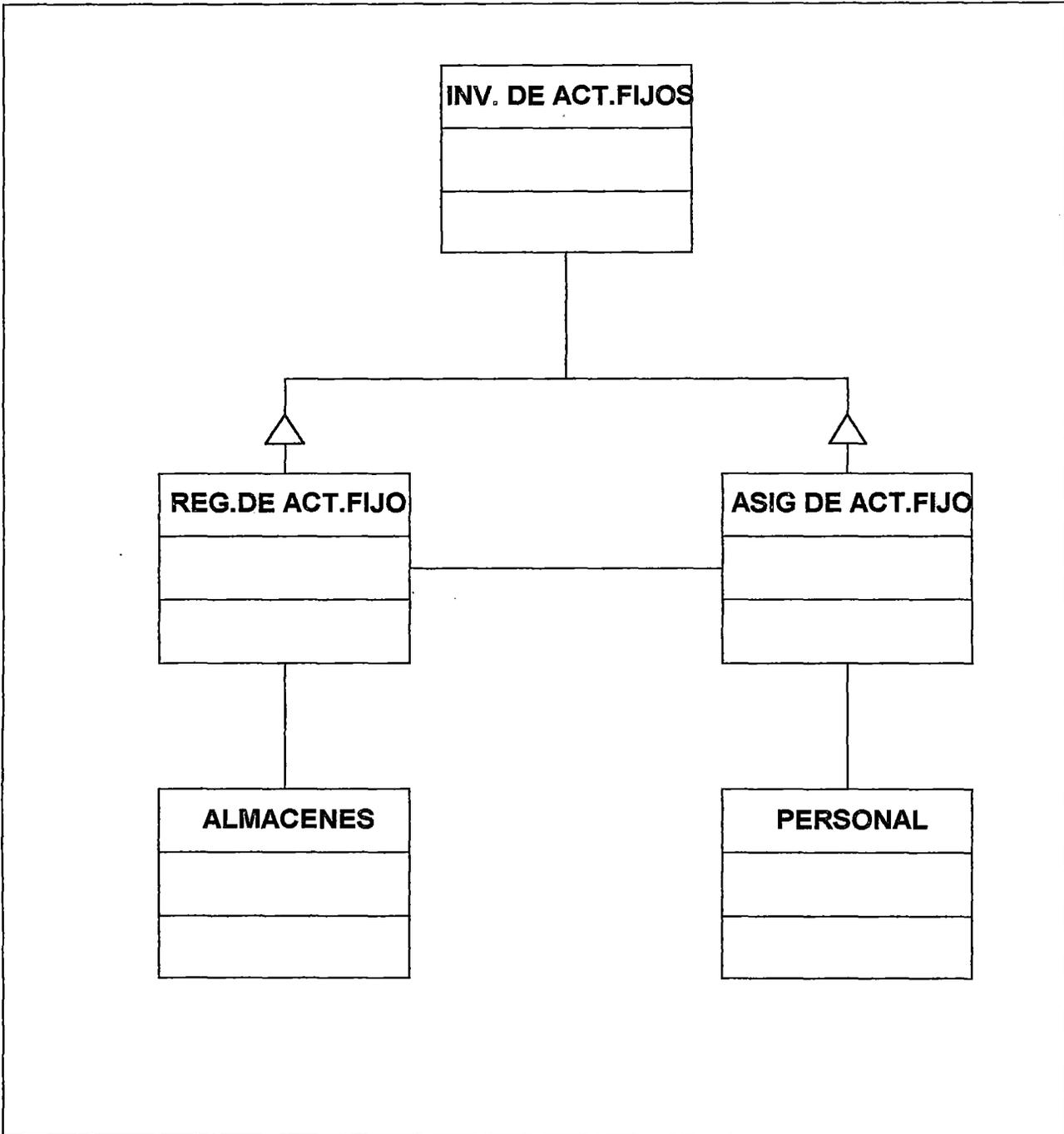


Figura 7

Como activo fijo, al bien en particular cuya Alta se registra, se le asigna un código único de activo fijo, el cual lo identificará durante toda su vida útil, hasta su baja correspondiente. Este código impreso en una etiqueta adhesiva, debe colocarse en algún lugar visible del bien.

El registro de bajas se hace normalmente por las siguientes causas:

- Venta.
- Siniestro.
- Deterioro.
- Obsolescencia (*).
- Desmantelamiento.

(*) Se entiende por obsolescencia, como la pérdida de utilidad comparativa con el desarrollo de nuevos equipos y procesos, cambios en diseño, u otras causas no relacionadas con la condición física del activo.

El registro de Altas, y sobre todo el registro de Bajas debe de estar debidamente autorizado, por quien corresponda según el Reglamento de Poderes y Autorizaciones.

Contablemente las bajas se registran a su valor en libros menos el valor de rescate que se obtenga por su enajenación final.

5.2. Asignación de Activos Fijos

Todo activo fijo debe estar asignado a alguna área o Dpto. de la empresa, debiendo registrarse por cada asignación por lo menos la información siguiente:

- a. Código de activo fijo.
- b. Descripción de activo fijo
- c. Unidad o Dpto. al que se asigna el activo fijo.
- d. Responsable directo.
- e. Ubicación física.
- f. Estado de conservación del bien.
- g. Fecha de asignación.
- h. Fecha de desasignación (*).

(*) Se entiende por desasignación, el cambio de Unidad o Dpto, el cambio de responsable directo.

5.3. Inventarios de Activos Fijos

Este módulo permite la toma de inventarios periódicos, por lo menos una vez al año, que cubran el total de los activos fijos existentes, comprobando su existencia física y el estado de conservación del bien.

ANEXO N° 04

DESCRIPCION DEL SISTEMA DE INFORMACION ACADEMICA

Se encarga de la administración de la información relacionada con los cursos llevados por los alumnos de la Universidad y las notas que obtuvieron en ellos, con la finalidad de satisfacer los requerimientos para el inicio de nuevos períodos académicos y para llevar el control de la situación académica del estudiante.

Responsabilidades del sistema

- a) Emisión de documentación requerida durante un proceso de matrícula como: orden de mérito, Fichas de Matrícula y avance curricular, resúmenes de curso – sección con alumnos matriculados. Boletas de verificación de cursos matriculados. Actas tras concluir el período de reclamos.
- b) Ejecución de matrícula en línea (control de cursos agotados, ampliaciones y cruces de horarios).
- c) Verificación de matrícula según reglamento, mostrando las incongruencias.
- d) Administración de retiros de cursos por reglamento y retiros voluntarios solicitado vía OSA.
- e) Manejar los montos a pagar (adeudos), en los casos de pérdida de gratuidad por antigüedad o cursos desaprobados.
- f) Controlar el acceso de OSA para el ingreso de notas y modificaciones de promedios errados.

- g) Soportar los cambios de currícula.
- h) Procesar las convalidaciones de cursos para el caso de traslados: las regularizaciones de cursos y resultados de exámenes aplazados.
- i) Mantener información de egresados, bachilleres y titulados, y los de expulsiones y retiro total.
- j) Administrar información relativa a ingresantes, tales como asignación de códigos e inspección de homónimos.
- k) Emisión de carnés (biblioteca , universitario).
- l) Administrar datos personales de alumnos y profesores (dirección, teléfono, etc.), mientras se desenvuelvan en la institución.

Exclusiones

- a) El sistema no almacena notas de prácticas y exámenes, sino promedios finales.
- b) No elabora horario de los cursos.
- c) No establece las vacantes para los cursos.
- d) No asigna profesores a los cursos.
- e) No establece el número de secciones para un curso.
- f) No determina si un curso se dictará en periodo académico o no.
- g) No evalúa la validez de los reclamos, sólo se limita a procesar aquellos que han sido aceptados en OSA.

1. Diagrama de Contexto

En la Figura 8 mostramos el diagrama de contexto del Sistema de Administración académica, observamos que las entidades que interactúan con dicho sistema son:

DIAGRAMA DE CONTEXTO

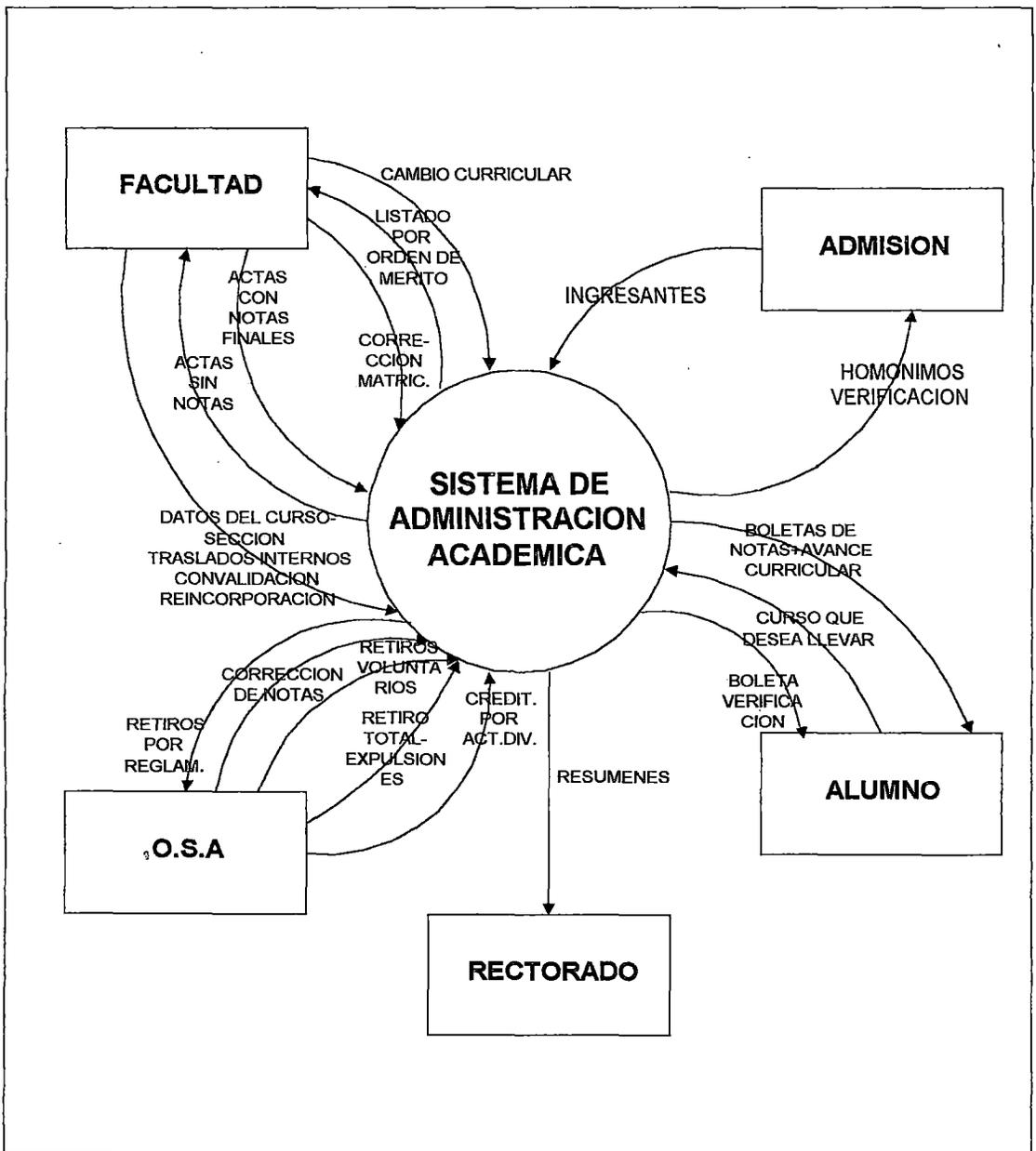


Figura 8

a) Las Facultades

Envían al sistema los cursos que se dictarán en el período académico, las secciones asociadas a éstos y las vacantes que existirán. Como evento extraordinario señalaremos que algunas facultades envían al sistema cambios curriculares en las especialidades.

También la lista de alumnos que realizaron traslado interno (mostrando las convalidaciones de cursos), los reincorporados.

Reciben una lista por orden de mérito para realizar el cronograma del proceso de matrícula y para que los alumnos conozcan el día que le corresponda matricularse.

También la lista de alumnos que realizaron traslado interno (mostrando las convalidaciones de cursos), los reincorporados y una lista por orden de mérito para realizar el cronograma del proceso de matrícula y para que los alumnos conozcan el día que le corresponde matricularse.

Las Facultades, además reciben actas que contienen los estudiantes matriculados en cada curso, y al terminar el periodo académico las devuelven con las notas finales de los alumnos.

b) La Oficina de Servicios Académicos (OSA)

Encargada de atender los reclamos de los alumnos y la responsable del buen funcionamiento del Sistema Académico.

Envía al sistema correcciones de notas, listas de alumnos retirados voluntariamente, retirados totalmente o, si es el caso, expulsados. También envía

al sistema la relación de estudiantes que recibirán créditos por actividades diversas.

Recibe del sistema, una relación de alumnos retirados por reglamento.

Ocasionalmente, si lo solicita, recibe los carnés impresos para ser sellados.

c) El Rectorado

Recibe algunos resúmenes como por ejemplo la relación de egresados en determinada facultad si lo solicita.

d) El Alumno

Previamente a un proceso de matrícula recibe su boleta de notas, avance curricular y ficha de matrícula. Durante la matrícula en sí, comunica al sistema los cursos que desea llevar. Posteriormente, recibe una boleta de verificación que le indica los cursos en que realmente está matriculado.

e) La Oficina de Admisión

Envía la relación de ingresantes por examen de admisión y traslado externo.

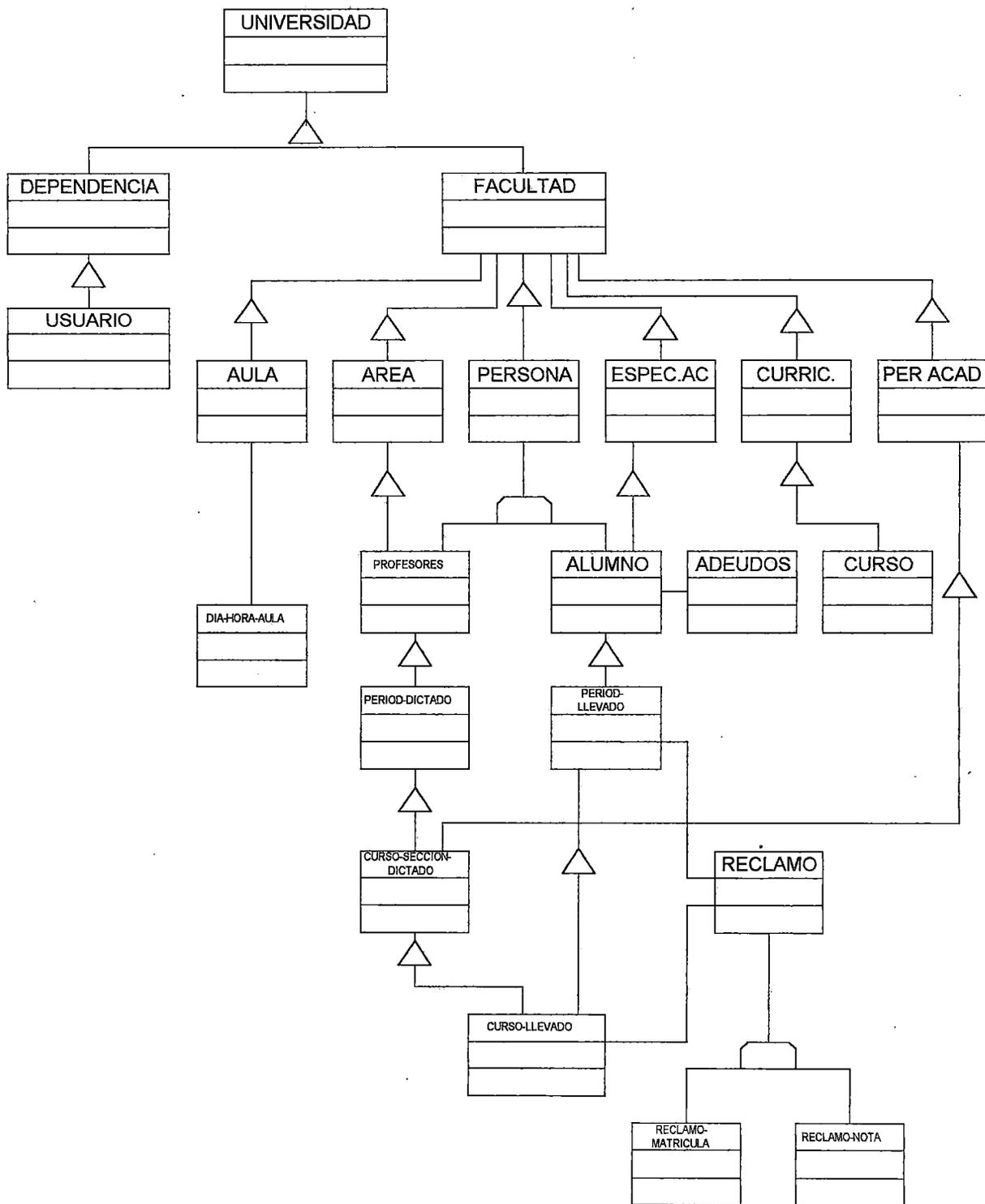
Recibe del sistema una lista de verificación de homónimos, esta lista se realiza para evitar que un alumno que ya ingreso a la universidad (probablemente no a la facultad que deseaba) vuelva ingresar al sistema.

2. Identificación de Clases y Objetos

Se han identificado la siguiente lista de objetos:

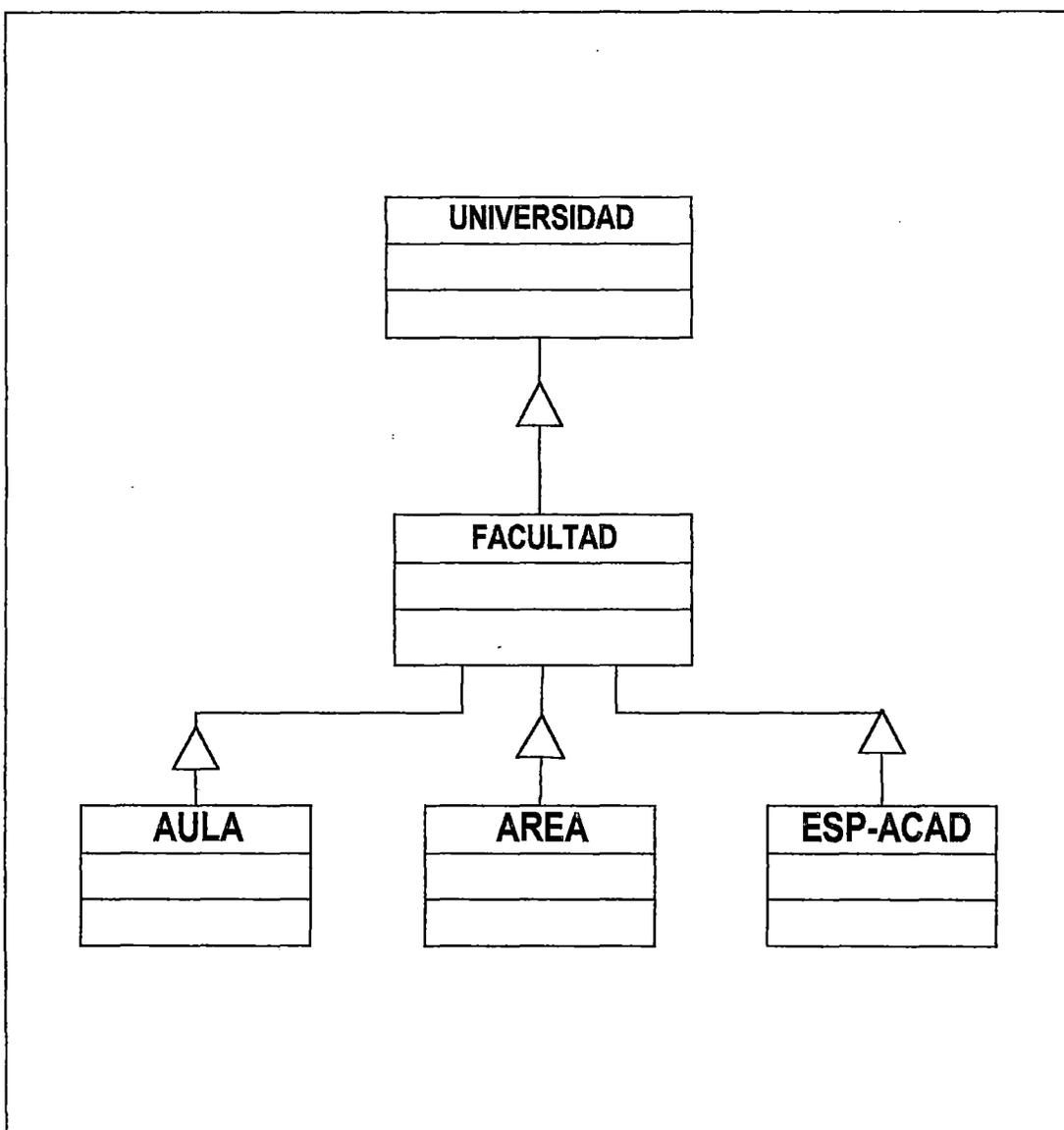
- | | |
|-----------------------------|---------------------------|
| a. Adeudos | - Período-Alumno |
| b. Alumno | - Período-Profesor |
| c. Alumno-Curso-Matriculado | - Proceso-Matrícula |
| d. Area | - Pre - requisito |
| e. Aula | - Profesor |
| f. Ficha-Académica | - Profesor-Curso-Dictando |
| g. Ficha-Estadística | - Regularización |
| h. Ficha-Postulante | - Reincorporación |
| i. Período-Actual | - Retiro-Total |
| j. Período-Académico | - Sanción |
| k. Aula-Día-Hora | - Título |
| l. Certificado | - Traslado-Interno |
| m. Curso-Llevado | - Universidad |
| n. Currícula | - Curso-Dictado |
| o. Curso-Sección-Dictado | - Curso-Sección-Actual |
| p. Curso | - Curso-Historia |
| q. Especialidad-Académica | - Estado-Curso-Curricular |
| r. Evento-Alumno | - Facultad |
| s. Ficha-Alumno | |

SISTEMA DE GESTION ACADEMICA

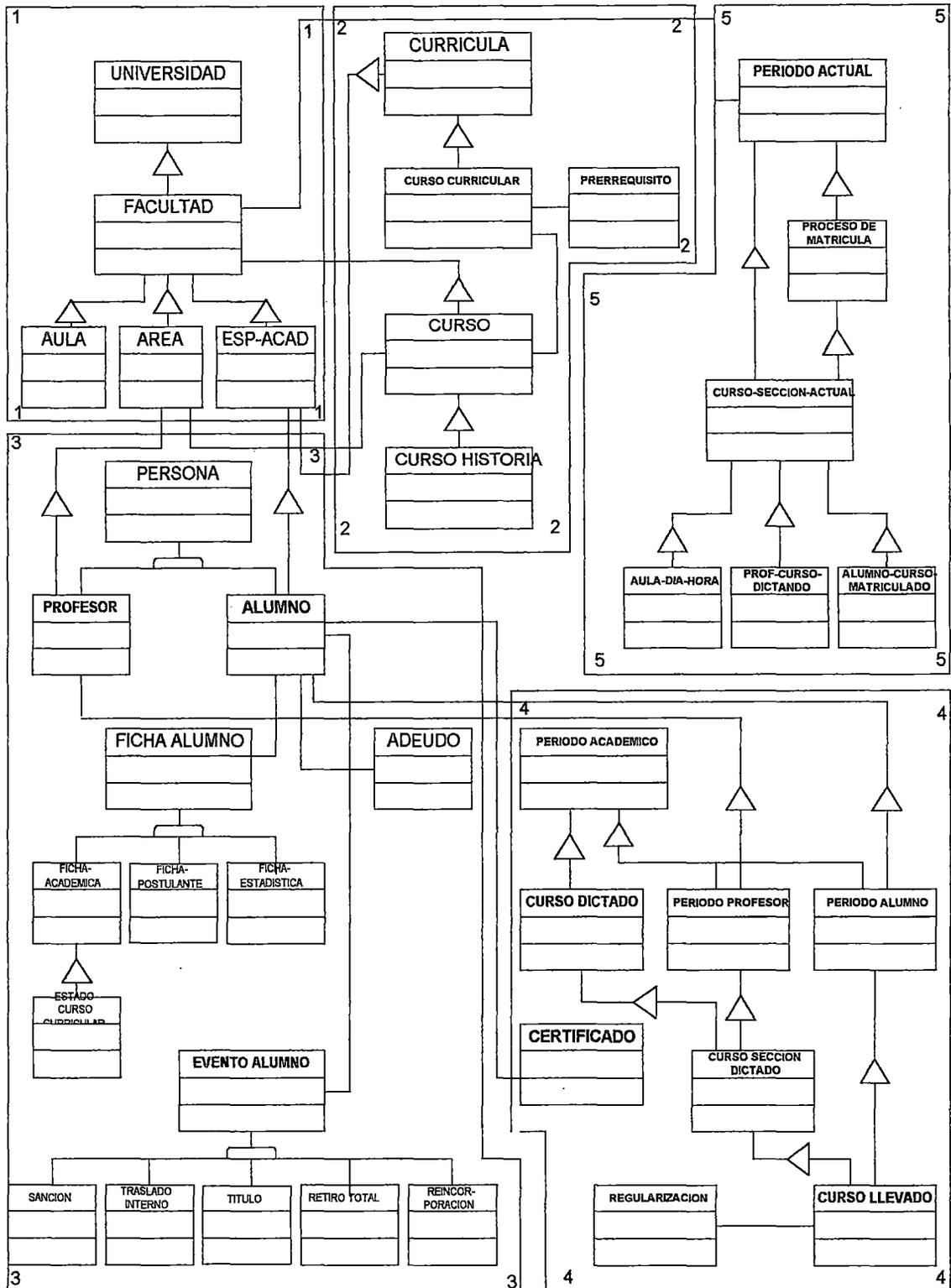


ESTRATO CLASE-&-OBJETOS Y ESTRUCTURA

OBJETO UNIVERSIDAD

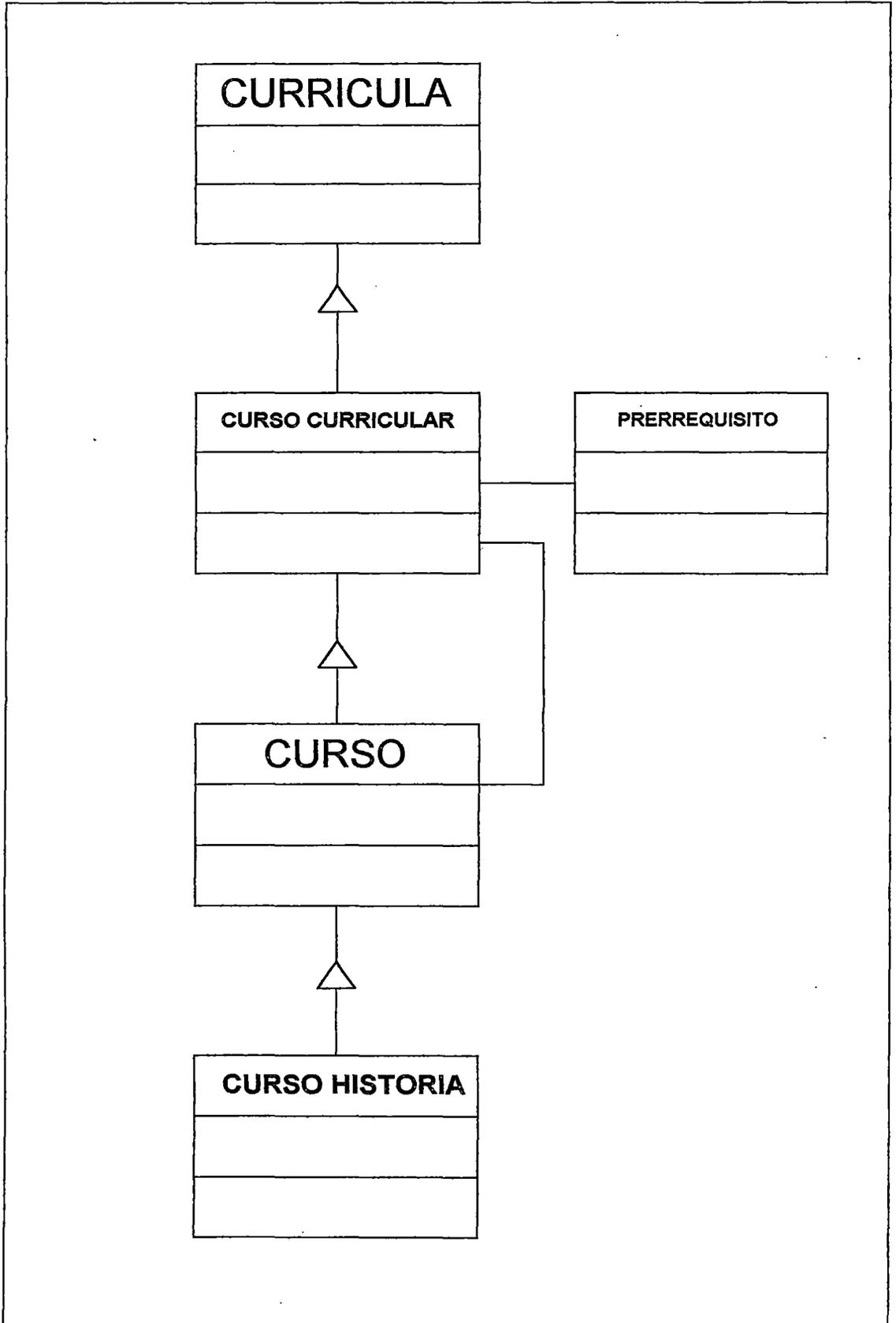


SISTEMA DE ADMINISTRACION ACADEMICA

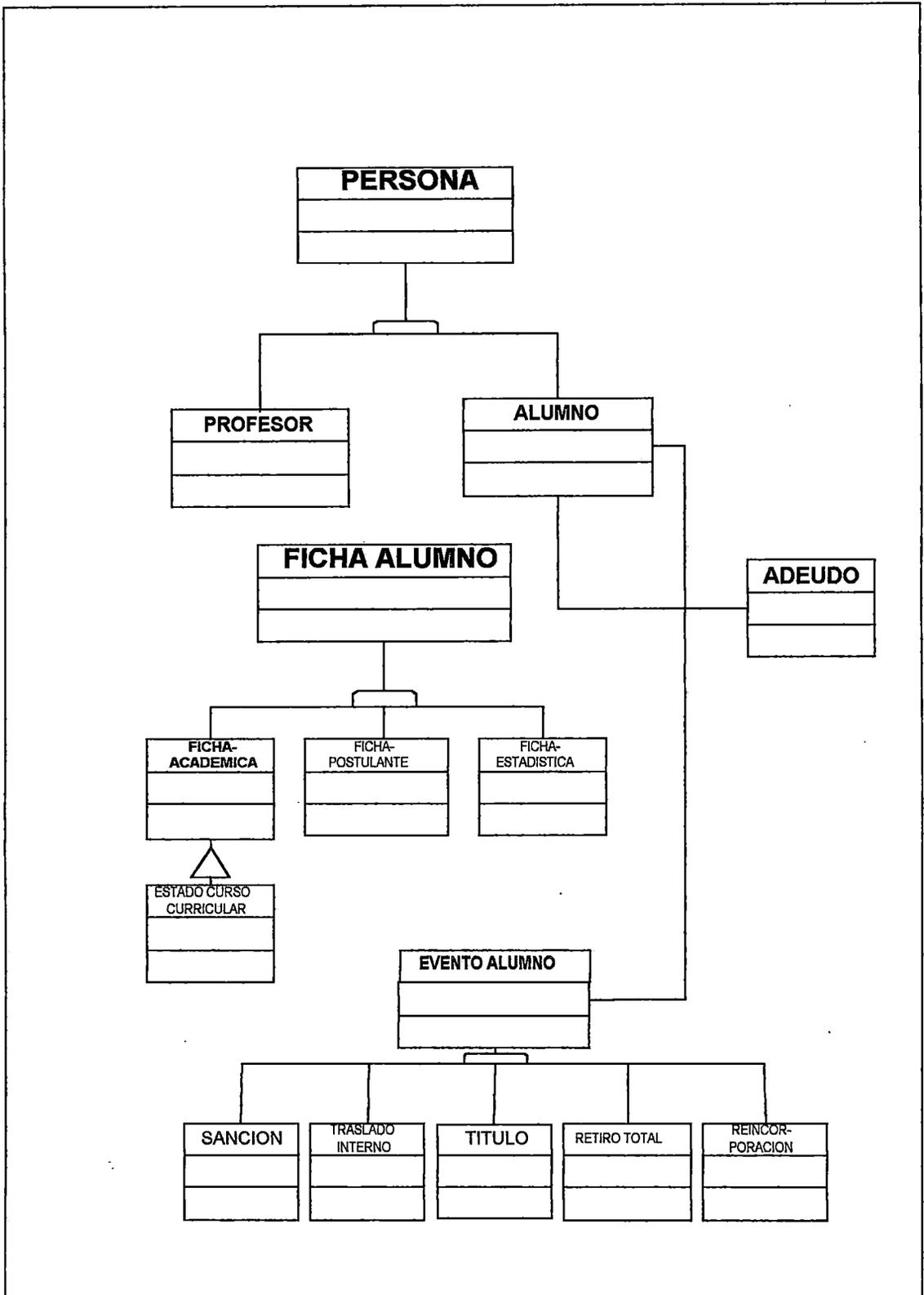


NIVELES CLASES-&OBJETO Y ESTRUCTURA

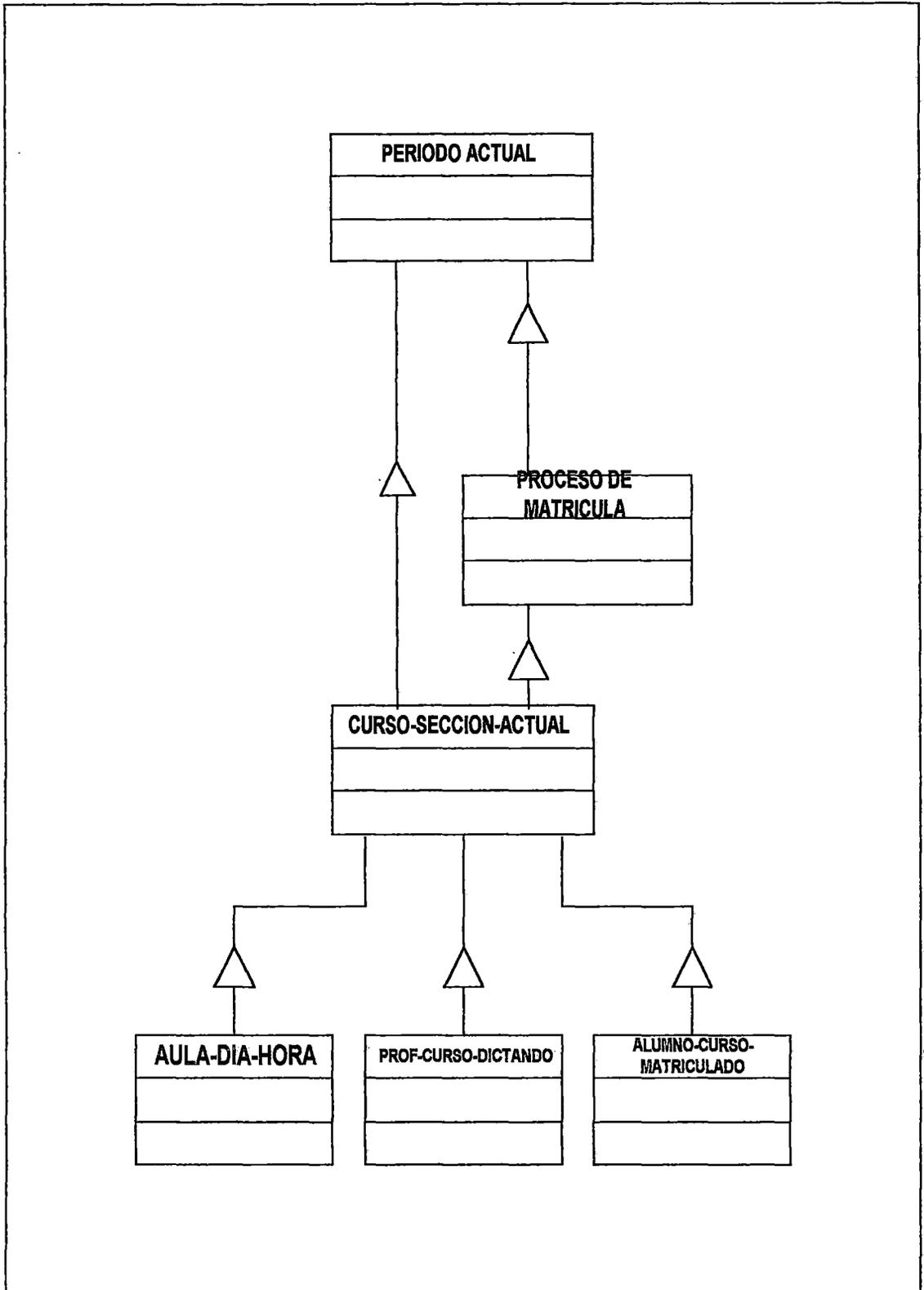
OBJETO CURRICULA



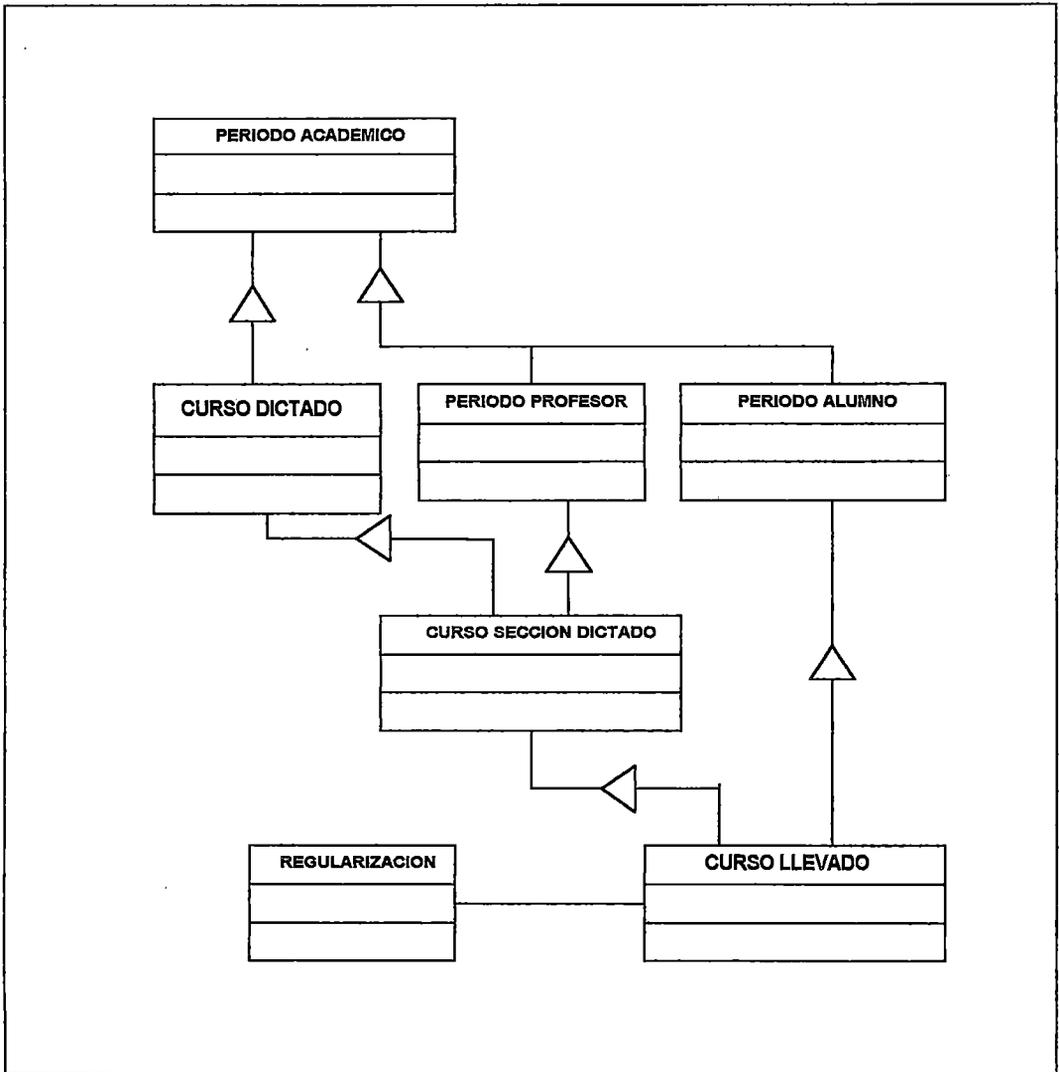
OBJETO PERSONA



OBJETO PERIODO ACTUAL



OBJETO PERIODO ACADEMICO



3. Identificación de Temas

Un Tema es un mecanismo para guiar al lector (analista, experto en el dominio del problema, gerente, cliente) a través de un modelo grande y complejo. Los temas son también útiles para organizar paquetes de trabajo en grandes proyectos, cuando previamente se han realizado las investigaciones del AOO.

La Figura muestra los temas identificados y los objetos comprendidos en cada uno de ellos. Estos temas son:

- a) Organización : Contiene todo los objetos que representan la organización académica.
- b) Curso-y-Currícula : Contiene a todos los objetos relacionados con el manejo de las currículas y los cursos contenidos en ellas.
- c) Persona : Contiene los objetos encargados de administrar la información general de las personas del sistema.
- d) Histórico : Contiene la información acumulada a través del tiempo en el sistema.
- e) Actualidad : Contiene información correspondiente a los periodos académicos actuales.

4. Identificación de Atributos

A continuación se muestran los atributos correspondientes a cada uno de los objetos reconocidos en el Dominio del Problema.

Objeto: Adeudo

Atributos :

Alumno	C(7)	* Código del Alumno
Especialidad	C(2)	* Código de la Especialidad
Dependencia	C(7)	* Código de la dependencia
Concepto	C(40)	* Concepto por el que se adeuda
Monto	N(15,2)	* Monto que se adeuda
Fecha	D(8)	* Fecha de creación del adeudo D(8)

Objeto: Alumno

Atributos :

Código	C(7)	* Código del alumno
Nombre	C(40)	* Nombre del alumno
Especialidad	C(2)	* Código de la especialidad
Situación	C(1)	* Situación del alumno (Normal, Bachiller,...)
Condición	C(1)	* Cond. Del alumno (Matriculado, Retirado,..)

Objeto: Alumno-Curso-Matriculado

Atributos :

Código	C(2)	* Código del Area
Facultad	C(1)	* Facultad del Area
Cod-Jefe-Area	C(7)	* Código del Jefe de Area
Nombre-Jefe	C(40)	* Nombre del Jefe del Area

Objeto: Alumno

Atributos :

Código	C(5)	* Código del Aula
Facultad	C(1)	* Código de facultad a que pertenece el aula
Capacidad	N(3)	* Capacidad del aula
Tipo	C(1)	* Tipo de aula (Salón, Laboratorio, Taller,....)

Objeto: Aula-Día-Hora

Atributos :

Aula	C(5)	* Código del Aula
Curso-Sección	C(7)	* Curso Sección a dictarse
Día	C(1)	* Día de la semana
Hora-Inicio	N(4)	* Hora y minutos Inicio de Clase
Hora-Fin	N(4)	* Hora y minutos Fin de Clase
Tipo-Hora	C(1)	* Tipo de hora (Teoría, Práctica, Laboratorio)

Objeto: Certificado

Atributos :

Alumno	C(7)	* Código del Alumno
Fecha-Ejec	D(8)	* Fecha de ejecución
Tipo	C(1)	* Tipo de Certificado (Depurado, No depurado)
Fecha-Impr	D(8)	* Fecha de Impresión
Num-Hojas	N(2)	* Número de hojas

Condición C(1) * Condición del certificado (Apto, No Apto)

Objeto: Curso-Llevado

Atributos:

Curso-Sección C(7) * Curso Sección Llevado

Alumno C(7) * Alumno que lleva el curso

Situación C(1) * Situación (Aprobado, Desaprobado, Sin Nota,...)

Tipo C(1) * Tipo (Obligatorio, Electivo, Extracurricular,..)

Condición C(1) * Condición (Normal, Convalidado, por Traslado,
Retiro, Exonerado,...)

Créditos N(2) * Créditos llevados

Nota P(99.9) * Nota que sacó el alumno

Semestre N(3) * Semestre en que llevó el Curso.

Objeto: Currícula

Atributos:

Especialidad C(2) * Especialidad de la currícula

Periodo-Inicial C(3) * Periodo Inicial

Periodo-Final C(3) * Periodo Final

Cred-Oblig N(3) * Número de créditos obligatorios

Cred-Elect N(3) * Número de créditos electivos

Cred-Compl N(3) * Número de créditos complementarios

Cred-Pre-Prof N(3) * Número de créditos Pre-Profesionales

Objeto: Curso Dictado

Atributos:

Código	C(6)	* Código del curso
Vacantes	N(3)	* Vacantes del Curso-Sección
Inscritos	N(3)	* Número de Inscritos
Sist-Eval	C(1)	* Sistema de Evaluación

Objeto: Curso-Sección-Dictado

Atributos:

Código	C(7)	* Código de Curso-Sección
Vacantes	N(3)	* Vacantes de Curso-Sección
Inscritos	N(3)	* Número de Inscritos
Ciclo-Matri	C(3)	* Ciclo de Matricula
Condición	C(1)	* Condición (Abierto, Separado en matrícula,..)
Sist-Eval	C(1)	* Sistema de Evaluación
Estado-Nota	C(1)	* Estado (Cargando Notas, No se ha Carg. Notas, Se ha terminado con errores, Proceso terminado,..)
Nota-Profesor	P(99.9)	* Nota del profesor Encuesta Docente.

Objeto: Curso-Sección-Actual

Atributos:

Código	C(7)	* Código del Curso Sección
Vacantes	N(3)	* Vacantes del Curso Sección

Inscritos	N(3)	* Número de Inscritos
Ciclo-Matri	C(3)	* Ciclo de Matricula
Condición	C(1)	* Condición (Abierto, Separado en matrícula)
Sist-Eval	C(1)	* Sistema de Evaluación
Estado-Nota	C(1)	* Estado (Cargando Notas, No se ha Carg. Notas, Se ha terminado con errores, Proceso terminado,..)

Objeto: Curso

Atributos:

Facultad	C(1)	* Facultad a la que pertenece
Cód-Curso	C(5)	* Código del curso
Nombre	C(40)	* Nombre del curso
Créditos	N(2)	* Créditos del curso
Condición	C(1)	* Condición (Dictado, No Dictado, Desaparecido)
Sist-Eval	C(1)	* Sistema de Evaluación
Horas-Teoría	N(2)	* Número de horas teoría
Horas-Pract	N(2)	* Número de horas de práctica
Horas-Labor	N(2)	* Número de horas de Laboratorio
Horas-Otros	N(2)	* Otras Horas
Período-Inicio	C(3)	* Período de Inicio
Objetivo	C(40)	* Objetivo del Curso C(40)
Syllabus	Memo	* Syllabus del curso

Objeto: Curso-Historia

Atributos:

Periodo-Inicio	C(3)	* Periodo de Inicio
Periodo-Fin	C(3)	* Período de Fin
Facultad	C(1)	* Facultad a la que pertenece
Cod-Curso	C(5)	* Código del Curso
Nombre	C(40)	* Nombre del Curso C(40)
Créditos	N(2)	* Créditos del curso
Sist-Eval	C(1)	* Sistema de Evaluación
Horas-Teoría	N(2)	* Número de horas teoría
Horas-Pract	N(2)	* Número de horas de práctica
Horas-Labor	N(2)	* Número de horas de Laboratorio
Horas-Otros	N(2)	* Otras Horas
Objetivo	C(40)	* Objetivo del Curso
Syllabus	Memo	* Syllabus del curso

Objeto: Especialidad-Académica

Atributos:

Código	C(2)	* Código de la especialidad
Nombre	C(40)	* Nombre de la especialidad
Título	C(1)	* Otorgado (Ingeniero, Bachiller,...)
Grado	C(1)	* Grado (Bachiller, Magister, Doctor,..)
Código - Jefe	C(7)	* Código jefe de escuela

Nombre – Jefe	C(40)	* Nombre jefe de escuela
Cred-Oblig	N(3)	* Créditos Obligatorios
Cred-Elect	N(3)	* Créditos Electivos
Cred-Compl	N(3)	* Créditos Complementarios

Clase: Estado-Curso-Curricular

Atributos:

Alumno	C(7)	* Alumno
Curso	C(6)	* Curso Curricular
Condición	C(1)	* Condición (Aprobado, Desaprobado)
Veces	N(2)	* Número de veces que llevó
Nota	P(99.9)	* Nota que tuvo

Clase: Evento-Alumno

Atributos:

Alumno	C(7)	* Alumno del evento
Fecha	D(8)	* Fecha en que ocurre

Objeto: Facultad

Atributos:

Código	C(1)	* Código del Facultad
Nombre	C(40)	* Nombre de la Facultad
Cód-Decano	C(7)	* Código del Decano

Nom-Decano	C(40)	* Nombre del Decano
Capac-Aulas	N(5)	* Capacidad de las Aulas
Num-Aulas	N(3)	* Número de Aulas

Clase: Ficha-Alumno

Atributos:

Alumno	C(7)	* Código del Alumno
Especialidad	C(2)	* Especialidad Académica
Per-Inicial	C(3)	* Período Inicial
Per-Final	C(3)	* Período Final
Per-Actualiz	C(3)	* Período de Actualización

Objeto: Ficha-Académica

Atributos:

Ciclo-Relativo	N(2)	* Ciclo Relativo
Mér-Llevado	N(5)	* Mérito Llevado
Mér-Aprov	N(5)	* Mérito Aprobado
Mér-Curr-Llev	N(5)	* Mérito Curricular llevado
Mér-Curr-Aprov	N(5)	* Mérito Curricular Aprobado
Prom-Pond-Ma	P(99.999)	* Promedio Matriculado
Prom-Pond-Ap	P(99.999)	* Promedio Aprobado
Prom-Curr-Mat	P(99.999)	* Promedio Curr. Matriculado
Prom-Curr-Ap	P(99.999)	* Promedio Curr. Aprobado

Cursos-Llev	N(3)	* Cursos Llevados
Cursos-Aprob	N(3)	* Cursos Aprobados
Cur-Curr-Llev	N(3)	* Cursos Curriculares Llevados
Cur-Curr-Aprob	N(3)	* Cursos Curriculares Aprobados
Cred-Llev	N(3)	* Créditos Llevados
Cred-Aprob	N(3)	* Créditos Aprobados
Cred-Curr-Llev	N(3)	* Créditos Curriculares Llevados
Cred-Curr-Ap	N(3)	* Créditos Curriculares Aprobados
Cred-Matri	N(3)	* Créditos Matriculados
Cred-Ap-Matri	N(3)	* Créditos Aprob. Matriculado
Cred-Curr-Mat	N(3)	* Créditos Curricular Matriculado
Cred-Curr-Ap-M	N(3)	* Créditos Curr. Aprob. Matric.

Objeto: Ficha-Estadística

Atributos:

Sexo	C(1)	* Sexo del Alumno
Estado-Civil	C(1)	* Estado Civil
Lugar-Nacim	C(60)	* País, Dpto, Provincia de Nacimiento
Fecha-Nacim	D(8)	* Fecha de Nacimiento
Doc-Identidad	C(10)	* Doc. Identidad (DNI, LE, LEM, Carnet de Extranjería.)
Domicilio	C(40)	* Domicilio Actual
Teléfono	C(6)	* Teléfono

Deudas N(15,2) * Deudas (De lab., de Biblioteca, por préstamo,...)

Ocupación C(1) * Ocupación (No trabaja, Dependiente, Indep,....)

Objeto: Ficha-Postulante

Atributos:

Tipo-Ingreso C(1) * Tipo (Admisión, Exonerado, Traslado, Externo,
Convenio Diplomático, Cepre,.....)

Veces-Postulo N(2) * Número de veces que postuló a la UANCV

Colegio-Egreso C(40) * Colegio que egreso

Tipo-Colegio C(1) * Tipo (Religioso, Laico, Nacional, Militar,.....)

Preparación C(1) * Tipo (Academia, Colegio, Autopreparación,...)

Objeto: Período-Actual

Atributos:

Código C(4) * Código del Período

Fecha-Ini D(8) * Fecha de Inicio

Alu-Norm N(5) * Alumnos Normales

Alu-Matr N(5) * Alumnos Matriculados

Objeto: Período-Académico

Atributos:

Código C(4) * Código del Período

Fecha-Ini D(8) * Fecha de Inicio

Fecha-Fin	D(8)	* Fecha de Fin
Condicion	C(1)	* Condición (Normal, Recesado, Especial, Vacacional, Nivelación, No programado,...)
Alu-Norm	N(5)	* Alumnos Normales
Alu-Matr	N(5)	* Alumnos Matriculados

Objeto: Período-Alumno

Atributos:

Per-Acd	C(4)	* Período Académico
Condición	C(1)	* Condición (Normal, Retoro total, No cursado, Suspend.)
Prom-Llev	P(99.999)	* Promedio Llevado
Prom-Aprob	N(3)	* Promedio Aprobado
Cursos-Llev	N(2)	* Cursos Llevados
Cred-Aprob	N(3)	* Créditos Aprobados
Especialidad	C(2)	* Código de la Especialidad
Ciclo-Relat	N(2)	* Ciclo Relativo

Objeto: Período-Profesor

Atributos:

Per-Acd	C(4)	* Período Académico
Promedio	P(99.999)	* Promedio de Encuestas

Objeto: Proceso-Matrícula

Atributos:

Per-Acd	C(4)	* Período Académico
Tipo	C(1)	* Tipo (Anual, Primer Semestre, Segundo Semes.)
Situación	C(1)	* (Prematricula, Matrícula, Verificación, retiros,..)
Día-Matrícula	N(2)	* Día de Matrícula

Objeto: Prerrequisito

Atributos:

Curso	C(6)	* Curso del cual es pre-requisito
Condición	C(1)	* (Pre-requisito, Co-prerrequisito)

Objeto: Profesor

Atributos:

Código	C(7)	* Código del Profesor
Nombre	C(40)	* Nombre del Profesor
Facultad	C(1)	* Facultad donde se enseña
Categoría	C(2)	* (Jefe de Práctica, Auxiliar, Asociado, Principal)
Dedicación	C(2)	* (Tiempo parcial, Completo, Exclusiva.)
Horas	N(2)	* Horas dedicadas
Situación	C(1)	* (Nombrado, Contratado)
Actividad	C(1)	* Actividad Actual (Dicta, Licencia, No dicta)
Oficina	C(5)	* Oficina del Profesor

Objeto: Profesor-Curso-Dictando

Atributos:

Profesor :	C(7)	* Código del Profesor
Cur-Sec	C(7)	* Curso-Sección dictando
Condición	C(1)	* (Teoría, Jefe de Práctica, Ayudante, Alumno)

Objeto: Regularización

Atributos :

Curso-Llevado	C(7)	* Curso Llevado
Alumno	C(7)	* Alumno que llevó el curso
Condición	C(1)	* (Regularización, Exonerado)
Período	C(3)	* Período de Regularización
Nota	P(99.9)	* Nota de Regularización
Fecha	D(8)	* Fecha de Regularización

Objeto: Reincorporación

Atributos:

Motivo	C(40)	* Motivo de Reincorporación
--------	-------	-----------------------------

Objeto: Retiro Total

Atributos:

Motivo	C(40)	* Motivo de la Interrupción
--------	-------	-----------------------------

Objeto: Sanción

Atributos:

Alumno	C(7)	* Código del Alumno
Especialidad	C(2)	* Especialidad del Alumno
Tipo-Docum	C(1)	* (Resolución rectoral, Proveído, Otros)
Num-Docum	C(4)	* Número de Documento
Fecha-Emisión	D(8)	* Fecha de Emisión
Texto-Sanción	C(120)	* Texto de Sanción
Vigencia	C(1)	* (No Vigente, Vigente, Sanción Temporal)
Condición	C(1)	* (Cumplió con la medida, Aun no se ejecuta)
Rec-Fecha	D(8)	* Fecha de Reconsideración
Rec-Texto	C(120)	* Texto de Reconsideración
Monto-Multa	N(15,2)	* Monto de la Multa

Objeto: Título

Atributos:

Descripción	C(40)	* Descripción del Título
-------------	-------	--------------------------

Objeto: Traslado-Interno

Atributos:

Espec-Anterior	C(2)	* Especialidad Anterior
Espec-Nueva	C(2)	* Especialidad Nueva
Cred-Conval	N(3)	* Créditos Convalidados

Objeto: Universidad

Atributos:

Nom-Rector	C(40)	* Nombre del Rector
Código	C(5)	* Código de la Universidad
Nombre	C(40)	* Nombre de la Universidad
Cód-Rector	C(7)	* Código del Rector

ANEXO N° 05

NORMAS GENERALES DEL PERÚ

- Constitución Política del Perú, artículos 81° y 82°.
- Ley del Sistema Nacional de Control -SNC; Decreto Ley N° 26162.
- Ley referida a la aplicación de la acción constitucional de Hábeas Data Ley N° 26301.
- Normas de Auditoría Generalmente Aceptadas - NAGA, aprobadas en el III Congreso Nacional de Contadores Públicos en 1997.
- Código Civil.
- Código Penal.
- Decreto Legislativo N° 604 Sistema Nacional de Informática... Estado”.
- Decreto Legislativo N° 768 “Valor Probatorio del Documento Informático”.
- Decreto Legislativo N° 681.
- Reglamento del Decreto Legislativo N° 681 D.S. 009-92-JUS “Sobre Microarchivos empresariales organizados con la tecnología de las microformas, mediante procesos de microfilmación por medios fotoquímicos y electrónicos”.
- Decreto Legislativo N° 822 “Ley Sobre el Derecho de Autor”.
- Decreto Ley N° 25868 “Ley de Organización y Funciones del Instituto Nacional de Defensa de la Competencia y Protección de la Propiedad Intelectual” de 24.NOV.92.
- Decreto Legislativo N° 807 “Facultades, Normas y Organización del INDECOPI”.

ANEXO N° 06

NORMAS Y DISPOSICIONES DE LA CONTRALORÍA

GENERAL DE LA REPÚBLICA -CGR

- Normas de Auditoría Gubernamental - NAGU, aprobado con Resolución de Contraloría N° 162-95-CG de 22.SET.95 y modificada mediante Resoluciones de Contraloría N° 246-95-CG de 28.DIC.95 y N° 112-97-CG de 20.JUN.97.
- Directiva N° 018-96-CG/CE “Lineamientos para el ejercicio de la auditoría interna en las entidades sujetas al ámbito de control”.
- Resolución de Contraloría N° 072-98-CG “Aprueban Normas Técnicas de Control Interno para el Sector Público”.
- Resolución de Contraloría N° 202-97-CG que aprueba la Directiva N° 007-97 referente a la “Presentación Sistematizada de Información, por parte de las Entidades sujetas al Sistema Nacional de Control”.
- Directiva N° 012-98-CG/PLF de 09.NOV.98 sobre: Lineamientos de Política y Directiva sobre el Plan Anual de Auditoría Gubernamental de los Órganos de Auditoría Interna, aprobado con Resolución de Contraloría N°135-98-CG.
- Manual de Auditoría Gubernamental - MAGU de 23.DIC.98.
- Guía para el Planeamiento de la Auditoría Gubernamental de 24.DIC.98.
- Guía para la Elaboración del Informe de Auditoría Gubernamental de 24.DIC.98.
- Guía de Papeles de Trabajo de 24.DIC.98.

ANEXO N° 07

NORMAS DEL INSTITUTO NACIONAL DE DEFENSA DE LA

COMPETENCIA Y PROTECCION DE LA PROPIEDAD

INTELECTUAL - INDECOPI

- Resolución N° 0121-1998/ODA-INDECOPI “Aprueban lineamientos de la Oficina de Derechos de Autor sobre el Uso Legal de los Programas de Ordenador (software) de 09.JUL.98.

ANEXO N° 08

NORMAS DEL INSTITUTO NACIONAL DE ESTADISTICA E **INFORMÁTICA - INEI**

- Resolución Jefatural N° 340-94-INEI, donde aprueba la Directiva N° 015-94-INEI/SJI “Normas Técnicas para el almacenamiento y respaldo de la información que se procesa en las Entidades del Estado” de 21.OCT.94.

- Resolución Jefatural N° 362-94-INEI, donde aprueba la Directiva N° 016-94-INEI/SJI “Normas para la prevención, detección y eliminación de virus informático en los equipos de computo de la Administración Publica” de 30.NOV.94.

- Resolución Jefatural N° 076-95-INEI, donde aprueba la Directiva N° 007-95-INEI/SJI “Recomendaciones Técnicas para la Seguridad e Integridad de la Información que se procesa en la Administración Publica” de 15.MAR.95.

- Resolución Jefatural N° 090-95-INEI, donde aprueba la Directiva N° 008-95-INEI/SJI “Recomendaciones Técnicas para la Protección Física de los Equipos y Medios de Procesamiento de la Información en la Administración Publica” de 30.MAR.95.

- Resolución Jefatural N° 140-95-INEI, donde aprueba la Directiva N° 010-95-INEI/SJI “Recomendaciones Técnicas para la Organización y Gestión de los Servicios Informáticos para la Administración Pública” de 08.JUN.95. Resolución Jefatural N° 154-95-INEI, de 27.JUN.95 donde se crea el Centro de Consulta e Investigación sobre virus Informáticos para la Administración Pública.

- Resolución Jefatural N° 229-95-INEI, de 14.SET.95 donde aprueba la Directiva N° 011-95-INEI/SJI “Recomendaciones Técnicas para la Elaboración de Planes de Sistemas de Información en la Administración Pública”.

ANEXO N° 09

DESCRIPCION ISACA

Un líder reconocido globalmente en control y seguridad de T.I.

Con más de 19.000 miembros en 100 países, la Asociación de Auditoría y Control en Sistemas de Información ISACA es un líder reconocido mundialmente en control y seguridad de Tecnologías de Información.

Fundada en 1969, ISACA auspicia conferencias nacionales e internacionales, administra globalmente la rendición del examen de certificación mundial CISA (Certified Information Systems Auditor) y desarrolla globalmente Standares de Auditoría y Control en Sistemas de Información.

La Misión de ISACA se basa en promover, mejorar y desarrollar las capacidades de nuestros asociados y de la comunidad en lo relacionado con la auditoría, seguridad, control y/o consultoría gerencial , en el campo de los sistemas y tecnologías de información.

Para cumplir plenamente con nuestra misión, pretendemos desarrollar fuertes y transparentes relaciones con el mundo académico participando activamente en carreras de Pregrado, Postítulos o Magister de nuestro ámbito. A su vez, nuestro contacto empresarial a niveles ejecutivos nos permitirá desarrollar en conjunto, por medio de

talleres u otro tipo de eventos las mejores prácticas en Seguridad y Control de Sistemas de Información.

Por ultimo, para cumplir con la Política de Educación Continua, para los Auditores CISA, la Asociación desarrollará Seminarios de interés en base a las necesidades del medio tecnológico.

STANDARES

La Asociación de Auditoría y Control de Sistemas de Información ha determinado que la naturaleza especializada de la auditoría de los sistemas de información y las habilidades necesarias para llevar a cabo este tipo de auditorías, requieren el desarrollo y la promulgación de Normas Generales para la Auditoría de los Sistemas de Información.

La auditoría de los sistemas de información se define como cualquier auditoría que 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.

Las normas promulgadas por la Asociación de Auditoría y Control de Sistemas de Información son aplicables al trabajo de auditoría realizado por miembros de la

Asociación de Auditoría y Control de Sistemas de Información y por las personas que han recibido la designación de Auditor Certificado de Sistemas de Información.

OBJETIVOS

Los objetivos de estas normas son los de informar a los auditores del nivel mínimo de rendimiento aceptable para satisfacer las responsabilidades profesionales establecidas en el Código de Ética Profesional y de informar a la gerencia y a otras partes interesadas de las expectativas de la profesión con respecto al trabajo de aquellos que la ejercen.

ANEXO N° 10

NORMAS GENERALES PARA LOS SISTEMAS DE

AUDITORÍA DE LA INFORMACIÓN

1. Título de auditoría

1.1 Responsabilidad, autoridad y rendimiento de cuentas

La responsabilidad, la autoridad y el rendimiento de cuentas abarcados por la función de auditoría de los sistemas de información se documentarán de la manera apropiada en un título de auditoría o carta de contratación.

2. Independencia

2.1 Independencia profesional

En todas las cuestiones relacionadas con la auditoría, el auditor de sistemas de información deberá ser independiente de la organización auditada tanto en actitud como en apariencia.

2.2 Relación organizativa

La función de auditoría de los sistemas de información deberá ser lo suficientemente independiente del área que se está auditando para permitir completar de manera objetiva la auditoría.

3. Ética y normas profesionales

3.1 Código de Ética Profesional

El auditor de sistemas de información deberá acatar el Código de Ética Profesional de la Asociación de Auditoría y Control de Sistemas de Información.

3.2 Atención profesional correspondiente

En todos los aspectos del trabajo del auditor de sistemas de información, se deberá ejercer la atención profesional correspondiente y el cumplimiento de las normas aplicables de auditoría profesional.

4. Idoneidad

4.1 Habilidades y conocimientos

El auditor de sistemas de información debe ser técnicamente idóneo, y tener las habilidades y los conocimientos necesarios para realizar el trabajo como auditor.

4.2 Educación profesional continua

El auditor de sistemas de información deberá mantener la idoneidad técnica por medio de la educación profesional continua correspondiente.

5. Planificación

5.1 Planificación de la auditoría

El auditor de sistemas de información deberá planificar el trabajo de auditoría de los sistemas de información para satisfacer los objetivos de la auditoría y para cumplir con las normas aplicables de auditoría profesional.

6. Ejecución del trabajo de auditoría

6.1 Supervisión

El personal de auditoría de los sistemas de información debe recibir la supervisión apropiada para proporcionar la garantía de que se cumpla con los objetivos de la auditoría y que se satisfagan las normas aplicables de auditoría profesional.

6.2 Evidencia

Durante el transcurso de una auditoría, el auditor de sistemas de información deberá obtener evidencia suficiente, confiable, relevante y útil para lograr de manera eficaz los objetivos de la auditoría. Los hallazgos y conclusiones de la auditoría se deberán apoyar por medio de un análisis e interpretación apropiados de dicha evidencia.

7. Informes

7.1 Contenido y formato de los informes

En el momento de completar el trabajo de auditoría, el auditor de sistemas de información deberá proporcionar un informe, de formato apropiado, a los destinatarios en cuestión. El informe de auditoría deberá enunciar el alcance, los objetivos, el período de cobertura y la naturaleza y amplitud del trabajo de auditoría realizado. El informe deberá identificar la organización, los destinatarios en cuestión y cualquier restricción con respecto a su circulación. El informe deberá enunciar los hallazgos, las conclusiones y las recomendaciones, y cualquier reserva o consideración que tuviera el auditor con respecto a la auditoría.

8. Actividades de seguimiento

8.1 Seguimiento

El auditor de sistemas de información deberá solicitar y evaluar la información apropiada con respecto a hallazgos, conclusiones y recomendaciones relevantes anteriores para determinar si se han implementado las acciones apropiadas de manera oportuna.

Fecha de vigencia: 25 de julio de 1997

Copyright © 1998 by the Information Systems Audit and Control Association. All rights reserved