UNIVERSIDAD NACIONAL DE INGENIERIA

Facultad de Ingeniería Industrial y de Sistemas

PROCESO DE AUDITORIA DE UN CENTRO DE PROCESAMIENTO DE INFORMACION DEL INTERIOR DEL PAIS

Informe de Ingeniería para optar el título de :

INGENIERO DE SISTEMAS

Presentado por :

MAXIMO IGNACIO PLASENCIA EZAINE

Lima - Perú
1996

DEDICATORIA

"A mis padres : Máximo y Mariela, por su esfuerzo y sacrificio, aliento y apoyo, infundiendo en mi la constancia para la culminación de mi carrera profesional y el deseo de superación"

"A mi futuro hijo y a mi esposa Liliana por su amor, comprensión y resuelto apoyo para la culminación de mis estudios profesionales"

"A Dios y a la Virgen por iluminarme cada día, guiándome por el camino del bien en la realización de mis metas trazadas"

ÍNDICE

SUMARIO

La Auditoría de Sistemas se desarrolló como respuesta al uso de las tecnologías de información, es por ello que los auditores de sistemas prueban los sistemas en busca de problemas de seguridad, identificando los riesgos y exposiciones de las tecnologías emergentes, desarrollando al mismo tiempo controles para reducir estos riesgos.

El Auditor de Sistemas debe realizar un proceso de auditoría más eficiente y eficaz, mejorando los procedimientos de auditoría mediante un adecuado planeamiento con un mayor enfoque en el análisis y evaluación de riesgos. El objetivo es rediseñar los procedimientos de auditoría, basándose en los estándares desarrollados por asociaciones profesionales existentes en el mundo.

Todo Proceso de Auditoría no tiene razón de ser, si es que no se realiza un seguimiento de las recomendaciones sugeridas en el mismo, constituyendo éstas recomendaciones un indicador que va a permitir comprobar si se han tomado las medidas correctivas adecuadas.

DESCRIPTORES TEMÁTICOS

1. Auditoría de Sistemas
2. Seguridad de la Información
3. Centro de Procesamiento de la Información
4. Ciclo de Vida de los Sistemas
5. Sistemas de Recaudación

INTRODUCCIÓN

Numerosos autores afirman que el mundo estaría alejándose de la era industrial para comenzar otra a la que se le ha bautizado como "de la información", caracterizada por una fuerte competencia, el rápido desarrollo tecnológico y la existencia de clientes y consumidores cada vez más informados, y por lo tanto más exigentes. Lo más importante para las empresas será la capacidad de adaptarse a un cambio constante y rápido, aprovechando al máximo la información que lo suministra el entorno que lo rodea.

Los cambios tecnológicos han traído como consecuencia una reducción de los costos de los equipos de cómputo, pero al mismo tiempo, la capacidad de procesamiento de los mismos se ha elevado notablemente. Los principales cambios tecnológicos se han dado en tres áreas: Hardware, Software y Ubicación Física del Centro de Procesamiento de la Información.

Sin embargo, estos cambios tecnológicos han estado acompañados por cambios conceptuales en los procedimientos de auditoría, lo que ha originado la especialización y la capacitación continua de los Auditores de Sistemas de Información, debido a que dichos cambios son cada vez más frecuentes.

Caso contrario sucede con los Sistemas de Control y Seguridad de la Información, los cuales no han avanzado a la misma velocidad que la Tecnología de la Información. La Reingeniería de Sistemas es una preocupación para los Auditores de Sistemas , como consecuencia de los

cambios constantes en los sistemas a fin de lograr una mayor eficiencia, motivo por el cual es necesario controlar estos cambios mediante la participación activa de los mismos.

El futuro de la Auditoría y Control de los Sistemas de Información, estará impulsado por sistemas cada vez más complejos, integradas mediante redes, permitiendo el uso de la información que apoye la toma de decisiones de la gerencia en un grado que nunca antes fue posible. Es por ello la necesidad de capacitar continuamente a los auditores, teniendo en cuenta el avance tecnológico y la subespecialización marcada por el giro del negocio. La labor realizada por los Auditores de Sistemas de Información no tiene sentido, sino se logra el compromiso y responsabilidad de la Alta Dirección de aceptar los riesgos inherentes al avance tecnológico.

El estudio del caso que a continuación se presenta, enfoca el desarrollo de una Metodología de Auditoría de Sistemas de Información que pueda ser aplicada en los diferentes Centros de Procesamiento de Información del Interior del País con que cuenta SUNAT. Como se sabe la SUNAT es una institución que ha evolucionado notablemente en los últimos 5 años, llegando a ser catalogada en estos momentos como la primera empresa del país.

Esta evolución ha estado acompañada por una elevada inversión en tecnología de la información, exigiendo un esfuerzo constante de evaluación debido al volumen de transacciones que se procesan diariamente. Esta evaluación es imposible realizarla bajo los esquemas de auditoría tradicional, siendo imprescindible la utilización del computador como una herramienta de apoyo en el Proceso de Auditoría.

La estructura del presente trabajo consta de tres capítulos:

- El Primer Capítulo, contiene el Perfil de la Empresa, el cual describe la Organizacional de SUNAT y la ubicación en el Organigrama de la Intendencia Nacional de Informática. Además, se describen las estrategias de SUNAT y los objetivos de los principales sistemas.
- El Segundo Capítulo, contiene el Marco Teórico de la Auditoría de Sistemas, describiendo los principales conceptos y las áreas de la organización donde se realiza el Proceso de Auditoría.
- El Tercer Capítulo, contiene la Aplicación Práctica, describiendo previamente el ambiente del Centro de Cómputo, para luego detallar las tareas que debe realizar el Auditor de Sistemas en cada una de las áreas involucradas. Luego vienen las Conclusiones, Recomendaciones, Bibliografia y los Anexos.

OBJETIVOS

El objetivo del presente trabajo es describir y recomendar los procedimientos a seguir por el Auditor de Sistemas para evaluar las actividades realizadas en el Centro de Procesamiento de Información con el propósito de detectar problemas que amenazen su operatividad o disminuyan su eficiencia, verificando los procedimientos de control y de seguridad, que nos permitan protegerlo de un acceso no autorizado.

ALCANCES

Los alcances a lograr con el presente trabajo son los siguientes:

1. Revisar el cumplimiento de políticas, normas y procedimientos institucionales en las áreas críticas del Centro de Procesamiento de Información.
2. Evaluar los controles incorporados en las principales aplicaciones, con el propósito de determinar la consistencia y confiabilidad de los mismos.
3. Verificar los controles que aseguren un procedimiento adecuado para el uso y resguardo de los activos fisicos y lógicos.

4. Evaluar los controles de acceso lógico y acceso físico; así como los controles dentro ambiente del centro de procesamiento de información.
5. Evaluar las operaciones realizadas en las instalaciones de centro de procesamiento de la información.

CAPITULO I : PERFIL DE LA EMPRESA

1.1 DE LA EMPRESA

1.1.1 MARCO LEGAL

La Superintendencia Nacional de Administración Tributaria se crea mediante Decreto Legislativo N° 771, el cual establece el Marco Legal del Sistema Tributario Nacional vigente.

1.1.2 OBJETIVO

Dotar al estado de los recursos económicos que le son necesarios para suministrar los servicios destinados a satisfacer las necesidades públicas, obteniendo tales recursos a través de la óptima orientación de los medios que intervienen en la Administración de los Procesos de Recaudación y Fiscalización de los tributos internos que la ley señale como competencia de Superintendencia Nacional de Administración Tributaria.

1.1.3 MISIÓN

Los trabajadores que conforman la Superintendencia Nacional de Administración Tributaria tienen la misión de dotar al estado de los recursos que le son necesarios, maximizando el cumplimiento voluntario de las obligaciones tributarias por parte de los contribuyentes.

Para la realizar lo mencionado anteriormente, es necesario hacer de la SUNAT una organización dinámica que se capaz de alcanzar sus objetivos al menor costo

posible (para SUNAT y para el contribuyente), compuesta por personal identificado con los valores de la institución y apto tanto moral como técnicamente para su labor tributaria, que desarrolle conciencia tributaria entre los ciudadanos, genere riesgo ante el incumplimiento tributario mediante su capacidad de control y, en todo momento, brinde un buen servicio al contribuyente.

Esta es la única manera de hacer a SUNAT una institución que contribuya a la construcción de un estado moderno, capaz de desarrollar eficientemente su rol de garante de una mejor vida en sociedad.

1.1.4 FUNCIONES GENERALES DE LA SUPERINTENDENCIA NACIONAL DE ADMINISTRACIÓN TRIBUTARIA

Las funciones de la Superintendencia Nacional de Administración Tributaria vinculadas con los procesos de Recaudación y Fiscalización de los Tributos a su cargo, son las siguientes:

a) Administrar los procesos de Recaudación y Fiscalización de los tributos internos y resolver las reclamaciones que sobre éstos se presenten.
b) Establecer mecanismos de prevención y detección de la evasión tributaria.
c) Proponer al Ministro de Economía y Finanzas la reglamentación de las Normas Tributarias.
d) Conceder el aplazamiento y/o fraccionamiento para el pago de la deuda tributaria.
e) Ejercer los actos de coerción para el cobro de la deuda tributaria mediante el ejecutor coactivo competente y efectuar el remate de los bienes decomisados y/o embargados en el ejercicio de sus funciones.
f) Resolver en primera instancia administrativa los recursos interpuestos por los contribuyentes o responsables respectos a los actos de Superintendencia Nacional de Administración Tributaria; conceder los recursos de apelación,

dar cumplimiento a las resoluciones del tribunal fiscal y en su caso, las del Poder Judicial.

g) Solicitar a cualquier autoridad competente, ejecutar conforme a la ley de la materia, medidas precautelatorias destinada a garantizar el pago de los tributos.

h) Emitir opinión respecto a los Proyectos de Acuerdos y Convenios Internacionales que celebre el Poder Ejecutivo cuando el ámbito de alcance del convenio esté relacionado con los fines de Superintendencia Nacional de Administración Tributaria.

i) Celebrar acuerdos de Cooperación Técnica y Administrativa en materia tributaria, con agencias y organismos internacionales a nombre propio y en representación del Supremo Gobierno. En este segundo caso, ejerce la representación cuando el ámbito de alcance del convenio esté relacionado con los fines institucionales.

j) Diseñar y desarrollar programas de información en materia tributaria.

k) Nombrar al Procurador Público encargado de los asuntos de Superintendencia Nacional de Administración Tributaria, para los casos de ley.

l) Otras funciones que sean compatibles con los fines de Superintendencia Nacional de Administración Tributaria.

1.1.5 ESTRUCTURA ORGÁNICA

Para el cumplimiento de sus fines la Superintendencia Nacional de Administración Tributaria cuenta con la siguiente estructura organizacional:

a) Alta Dirección

Superintendente Nacional de Administración Tributaria

Superintendente Nacional Adjunto de Administración Tributaria

b) Órganos de Apoyo

Secretaria General

Oficina Nacional de Comunicaciones

Instituto de Administración Tributaria

Oficina Nacional de Atención al Contribuyente

c) Órganos de Control

Oficina de Control Interno

d) Entidad Adscrita

Unidad Especial de Investigaciones Tributarias

e) Órganos de Línea

Intendencia Nacional de Desarrollo Tributario

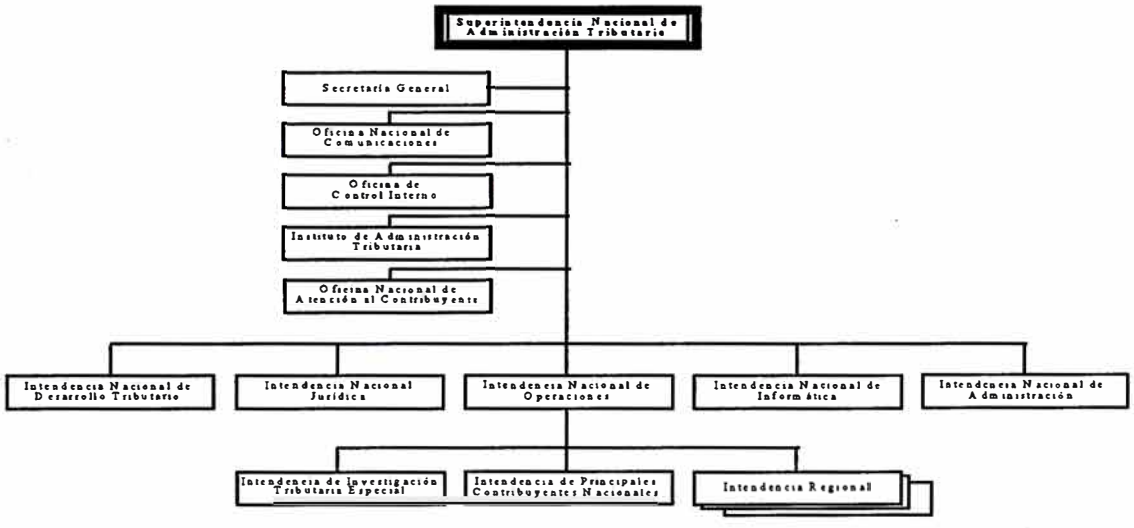
Intendencia Nacional Jurídica

Intendencia Nacional de Operaciones

Intendencia Nacional de Informática

Intendencia Nacional de Administración

Figura 1.1 : Organigrama de SUNAT



Cuadro 1.1 : Organismos Descentralizados

Intendencia Regional	*Oficina Zonal*	
	Tipo A	*Tipo B*
Lima	Huacho	
Arequipa	Puno	
Cusco		Apurímac Madre de Dios
Ica		Cañete Ayacucho
Junín	Huánuco	Pasco Huancavelica
La Libertad	Chimbote	Huaraz
Lambayeque	Cajamarca	Amazonas
Loreto	Ucayali San Martín	
Piura		Tumbes
Tacna	Moquegua	

Figura 1.2 : Estructura Organizacional de una Intendencia Regional

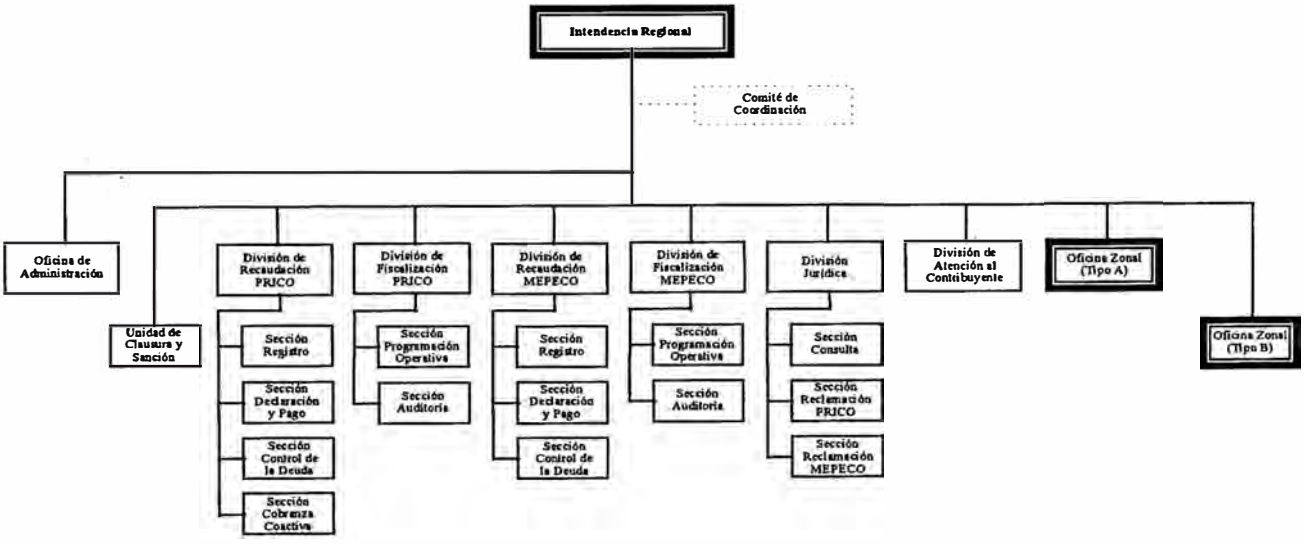


Figura 1.3 Estructura Organizacional de una Oficina Zonal Tipo A

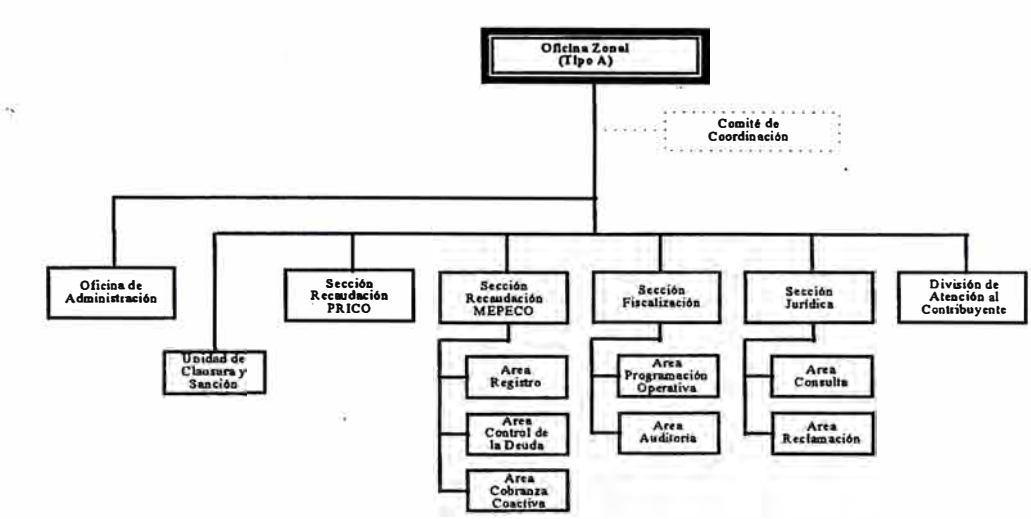
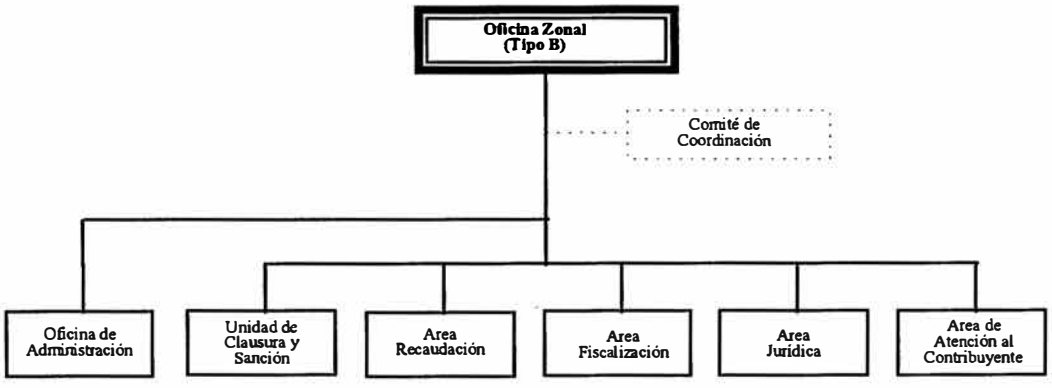


Figura 1.4 : Estructura Organizacional de una Oficina Zonal Tipo B



1.1.6 INTENDENCIA NACIONAL DE INFORMÁTICA

Objetivo:

Coadyuvar al logro de los objetivos de la SUNAT, manteniendo la eficiencia operativa de las unidades organizacionales que la conforman a través del permanente, oportuno y actualizado servicio informático.

Funciones:

a) Controlar el cumplimiento de las actividades de las gerencias que conforman la Intendencia Nacional de Informática.

b) Aprobar los planes de trabajo presentados por la Gerencia de Aplicaciones y por la Gerencia de Producción.

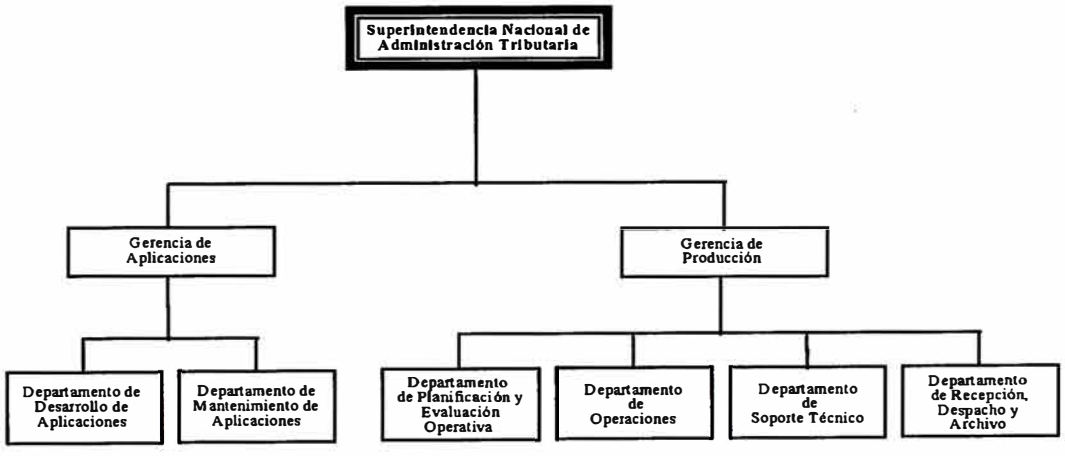
c) Aprobar el desarrollo de las aplicaciones informáticas para uso de la institución.

d) Establecer los lineamientos administrativos de los procesos que competen a la Intendencia Nacional de Informática.

e) Presentar propuestas sobre hardware y software que incorporen nuevas tecnologías que optimicen el desarrollo funcional de la institución.

f) Emitir circulares de su competencia.

Figura 5 : Estructura Organizacional de la Intendencia Nacional de Informática



1.1.6.1 GERENCIA DE APLICACIONES

Objetivo :

Asegurar el mayor rendimiento organizacional, a través de la sistematización de las actividades que se desarrollan en la institución, mediante la implantación de aplicaciones informáticas.

Funciones :

a) Controlar el cumplimiento de las actividades de los departamentos que conforman la Gerencia de Aplicaciones.

b) Producir el Plan Anual sobre el desarrollo de las aplicaciones.

c) Elaborar proyectos referidos a nuevas aplicaciones y/o modificaciones a las aplicaciones implantadas.

d) Presentar informes referidos al ciclo de vida de las aplicaciones desarrolladas.

e) Establecer normas para la operación de las aplicaciones.

f) Formular planes de capacitación del personal de la institución para el uso de las aplicaciones informáticas desarrolladas.

1.1.6.1.1 DEPARTAMENTO DE DESARROLLO DE APLICACIONES

Objetivo :

Desarrollar aplicaciones informáticas para facilitar y reducir tiempos en la ejecución de los trabajos que deben realizarse en las unidades organizacionales que conforman la institución.

Funciones :

a) Formular el plan anual de desarrollo de aplicaciones.

b) Presentar los proyectos de aplicaciones para el uso de la institución de acuerdo al plan aprobado.

c) Producir manuales de operación de las aplicaciones desarrolladas.

d) Elaborar la documentación técnica de las aplicaciones desarrolladas.

e) Efectuar el entrenamiento y capacitación del personal de la institución para el uso de las aplicaciones informáticas desarrolladas.

1.1.6.1.2 DEPARTAMENTO DE MANTENIMIENTO DE APLICACIONES

Objetivo :

Asegurar la vida útil de las aplicaciones informáticas de la institución, mediante acciones oportunas de su mantenimiento.

Funciones :

a) Ejecutar el mantenimiento de las aplicaciones informáticas desarrolladas para uso de la institución.

b) Producir informes respecto al ciclo de vida de las aplicaciones informáticas desarrollas.

c) Efectuar la actualización de la documentación técnica de las aplicaciones informáticas desarrolladas por el Departamento de Desarrollo de Aplicaciones.

d) Efectuar el entrenamiento y capacitación del personal de la institución, por los cambios que se realizan en las aplicaciones informáticas.

1.1.6.2 GERENCIA DE PRODUCCIÓN

Objetivo :

Asegurar el logro del objetivo de la Intendencia Nacional de Informática, facilitando a las unidades organizacionales de la institución la atención a sus requerimientos de procesamiento de datos con un efectivo y oportuno servicio informático.

Funciones :

a) Controlar el cumplimiento de las actividades de los Departamentos que conforman la Gerencia de Producción.

b) Presentar el Plan operativo anual de las unidades organizacionales que conforman la Gerencia de Producción.

c) Establecer normas para el control de la operación de los sistemas implantados en la institución.

d) Producir proyectos sobre hardware y software que incorporen el avance tecnológico que optimicen el desarrollo funcional de la institución.

e) Producir informes sobre especificaciones técnicas para la adquisición de hardware y software.

f) Administrar la operación continua de los Sistemas de Información operativa y administrativa que posee la institución.

1.1.6.2.1 DEPARTAMENTO DE PLANIFICACIÓN Y EVALUACIÓN OPERATIVA

Objetivo :

Asegurar que el logro de los objetivos de las unidades organizacionales que conforman la Gerencia de Producción se alcance con eficiencia y en forma ordenada y controlada, a través de la oportuna planificación y evaluación de sus actividades.

Funciones :

a) Formular el Plan Anual de Producción para la ejecución de las actividades de las unidades organizacionales que comprende la Gerencia de Producción.

b) Realizar y ejecutar el Plan Anual de Auditorías de los sistemas informáticos de la institución.

c) Formular el Plan Anual de Mantenimiento Preventivo a los equipos informáticos de la institución.

d) Elaborar las normas de control de la operación de las normas implantadas.

e) Efectuar el seguimiento de la carga operativa de las aplicaciones instaladas.

f) Producir informes sobre el grado de cumplimiento observado en el seguimiento de los planes anuales de producción, de mantenimiento y de auditoría de las aplicaciones.

g) Formular el Plan Anual de Control del Hardware y Software adquiridos por la SUNAT.

h) Formular, controlar y evaluar la ejecución del Plan de Contingencias Informáticas de SUNAT.

1.1.6.2.2 DEPARTAMENTO DE OPERACIONES

Objetivo :

Abastecer de información confiable y oportuna a las unidades organizacionales de la institución a partir del procesamiento de los datos suministrados.

Funciones :

a) Ejecutar el Plan Anual de Producción aprobado.

b) Generar y custodiar el respaldo (BackUp) de la información procesada.

c) Activar el sistema red de la institución de acuerdo a la normatividad vigente.

d) Custodiar, mantener y abastecer de los suministros informáticos y dispositivos magnéticos a las unidades organizacionales que comprende la Gerencia de Producción.

e) Custodiar y mantener la biblioteca de archivos de información y programas de los sistemas en producción.

1.1.6.2.3 DEPARTAMENTO DE SOPORTE TÉCNICO

Objetivo :

Mantener en buen estado operativo los equipos informáticos de la institución, a través de acciones oportunas de su mantenimiento y de orientación para su adecuada utilización.

Funciones :

a) Ejecutar el mantenimiento preventivo a los equipos informáticos de acuerdo al Plan Anual de Mantenimiento aprobado.

b) Ejecutar la Auditoría Informática referida al software base y hardware de los equipos adquiridos por la institución.

c) Producir proyectos que planteen la actualización de los equipos informáticos de la institución.

d) Instalar los equipos informáticos y software adquirido por la institución.

e) Difundir las técnicas de aprovechamiento de soportes informáticos entre los usuarios de la institución.

f) Determinar las especificaciones técnicas para la adquisición de hardware y software de la institución.

g) Autorizar el acceso a los sistemas informáticos de la institución.

h) Administrar la base de datos existente en la institución.

i) Autorizar el pase a producción de las aplicaciones desarrollada por la Gerencia de Aplicaciones y elaborar las normas para la atención de las mismas.

j) Mantener la interconexión de los diferentes equipos de la red informática de la institución.

1.1.6.2.4 DEPARTAMENTO DE RECEPCIÓN, DESPACHO Y ARCHIVO

Objetivo :

Asegurar la custodia temporal y conservación adecuada de la documentación de carácter tributario presentada por los contribuyentes en las entidades bancarias autorizadas y dependencias de la institución.

Funciones :

a) Custodiar y mantener la documentación de carácter tributario que se recepcionan en las entidades bancarias y dependencias de SUNAT de conformidad con la normatividad vigente.

b) Formular el Plan Anual de actividades de archivo periférico

c) Proporcionar los documentos en custodia de carácter tributario que requiera el Departamento de Operaciones de la Gerencia de Producción para su procesamiento.

d) Atender las solicitudes de fotocopiado de declaraciones juradas que formule la Sección de Archivo Central y otras unidades organizacionales autorizadas de la institución.

1.2 ESTRATEGIAS

Dado que la misión de SUNAT es dotar al estado de los recursos necesarios para que éste cumpla con sus objetivos, la política de la institución se basa en tres puntos básicos:

1. La creación de riesgo, la cual esta relacionada con las acciones de fiscalización, buscando seleccionar un mayor número de contribuyentes.
2. El desarrollo permanente de la conciencia tributaria, la cual debe partir de la base de nuestro cimiento educativo: los colegios, a fin de alcanzar frutos en el mediano plazo.
3. El mejoramiento de la calidad del servicio, el cual debe ser expresado en la elaboración de productos de calidad en cada departamento o sección.

Lo mencionado anteriormente ha permitido aumentar la recaudación nominal en 1995 en 26.8 % respecto a la registrada en 1994. Este incremento se debe principalmente al desempeño de las variables macroeconómicas esperadas, a los cambios realizados en la legislación tributaria, así como a las mejoras en los procedimientos administrativos.

Cuadro 1.2 : Metas de Recaudación

Dependencia	*1,994*		*1,995*	
	Parcial	*Total*	*Parcial*	*Total*
Intendencia de Principales Contribuyentes Nacionales		5,555,003		7,121,132
Intendencia Regional Lima	1,828,564		2,219,806	
Oficina Zonal Huacho	39,480	1,868,044	45,824	2,265,630
Intendencia Regional Arequipa	366,676		482,261	
Oficina Zonal Puno	18,696	385,372	28,045	510,306
Intendencia Regional Cusco	52,443		74,920	
Oficina Zonal Apurímac	2,901		3,622	
Oficina Zonal Madre de Dios	2,093	57,437	3,140	81,682
Intendencia Regional Ica	93,387		119,987	
Oficina Zonal Cañete	8,423		9,687	
Oficina Zonal Ayacucho	7,218	109,028	10,826	140,500
Intendencia Regional Junín	61,531		92,296	
Oficina Zonal Húanuco	9,455		13,485	
Oficina Zonal Pasco	6,007		8,242	
Oficina Zonal Huancavelica	2,784	79,777	4,110	118,133
Intendencia Regional La Libertad	210,721		280,700	
Oficina Zonal Chimbote	73,109		97,546	
Oficina Zonal Huaraz	4,777	288,607	6,654	384,900
Intendencia Regional Lambayeque	128,875		163,262	
Oficina Zonal Cajamarca	20,242		24,825	
Oficina Zonal Amazonas	2,120	151,237	2,978	191,065
Intendencia Regional Loreto	41,872		48,152	
Oficina Zonal Ucayali	21,154		31,086	
Oficina Zonal San Martín	13,123	76,149	19,657	98,895
Intendencia Regional Piura	105,118		136,033	
Oficina Zonal Tumbes	6,545	111,663	8,904	144,937
Intendencia Regional Tacna	77,102		113,917	
Oficina Zonal Moquegua	20,329	97,431	25,086	139,003
		8,779,748		**11,196,183**

Los contribuyentes inscritos que realizan pagos a Diciembre de 1995 se han incrementado a 444,720 contribuyentes, el cual es superior a los 354,812 de Diciembre de 1995 debido a al mayor control realizado a los nuevos contribuyentes, los cuales en 1994 registraron un ratio de pago relativamente bajo.

El ratio de contribuyentes que pagan entre los contribuyentes inscritos es de 40.3 % a Diciembre de 1995 frente a los 27.3 % de Diciembre de 1994. Este resultado toma en cuenta las bajas automáticas efectuadas en 1995.

El número de reclamos pendientes de resolver a Diciembre de 1995 es de 2780 expedientes, el cual es inferior a los 7818 registrados en Diciembre de 1994. Esta reducción se debe al mejoramiento continuo de los procedimientos administrativos y de la racionalización y mejor asignación de los recursos humanos existentes.

Las metas de fiscalización a Diciembre de 1995 son de 20862 auditorías, el cual es ligeramente superior a los 20276 auditorías realizadas en 1994. Es incremento se debe a al incremento de recursos humanos en la dependencias del interior del país.

Cuadro 1.3 : Relación de Contribuyentes que Pagan y Contribuyentes Inscritos

Dependencia	*Contribuyentes que Pagan*		*Contribuyentes Inscritos*		*Ratio*	
	1,994	*1,995*	*1,994*	*1,995*	*1,994*	*1,995*
Intendencia de Principales Contribuyentes Nacionales	1,478	1,641	1,632	1,641	0.906	1.000
Intendencia Regional Lima	184,612	234,424	684,753	604,778	0.270	0.388
Oficina Zonal Huacho	6,442	7,783	25,456	18,589	0.253	0.419
Intendencia Regional Arequipa	25,213	30,370	74,078	64,748	0.340	0.469
Oficina Zonal Puno	4,475	6,216	31,147	20,219	0.144	0.307
Intendencia Regional Cusco	10,789	13,983	43,568	33,704	0.248	0.415
Oficina Zonal Apurímac	1,547	1,874	5,602	4,292	0.276	0.437
Oficina Zonal Madre de Dios	653	855	2,801	2,316	0.233	0.369
Intendencia Regional Ica	12,154	14,319	38,354	30,980	0.317	0.462
Oficina Zonal Cañete	2,840	3,440	10,518	8,365	0.270	0.411
Oficina Zonal Ayacucho	2,870	3,416	8,449	7,228	0.340	0.473
Intendencia Regional Junín	14,285	17,708	45,133	39,640	0.317	0.447
Oficina Zonal Húanuco	3,736	4,800	19,851	13,091	0.188	0.367
Oficina Zonal Pasco	3,406	3,989	8,681	7,222	0.392	0.552
Oficina Zonal Huancavelica	1,340	1,844	4,173	7,059	0.321	0.261
Intendencia Regional La Libertad	16,959	21,017	63,786	49,939	0.266	0.421
Oficina Zonal Chimbote	5,895	7,362	21,200	17,697	0.278	0.416
Oficina Zonal Huaraz	2,875	3,488	10,719	8,104	0.268	0.430
Intendencia Regional Lambayeque	13,746	16,640	45,810	37,948	0.300	0.438
Oficina Zonal Cajamarca	4,455	5,320	13,957	11,711	0.319	0.454
Oficina Zonal Amazonas	1,850	2,160	4,705	4,284	0.393	0.504
Intendencia Regional Loreto	2,906	4,168	18,253	13,388	0.159	0.311
Oficina Zonal Ucayali	1,889	2,668	10,461	8,371	0.181	0.319
Oficina Zonal San Martín	3,729	4,859	15,318	12,469	0.243	0.390
Intendencia Regional Piura	13,902	17,012	51,118	42,484	0.272	0.400
Oficina Zonal Tumbes	2,110	2,462	6,574	5,504	0.321	0.447
Intendencia Regional Tacna	5,445	7,084	22,812	19,107	0.239	0.371
Oficina Zonal Moquegua	3,211	3,818	9,248	7,871	0.347	0.485
	354,812	**444,720**	**1,298,157**	**1,102,749**	**0.273**	**0.403**

1.3 OBJETIVOS

1.3.1 SISTEMAS DE RECAUDACION

1. Fomentar el Incremento de la Recaudación, a través de un eficiente sistema de control y cobranza de la deuda.
2. Mejorar la calidad en el otorgamiento del RUC. Disminuir el número de contribuyentes que tienen RUC y que no deben tenerlo.
3. Ampliar la base de contribuyentes inscritos, así como el Directorio de Principales Contribuyentes.
4. Verificar y actualizar continuamente el Padrón de Principales y Medianos Contribuyentes.
5. Crear un directorio de contribuyentes activos y pasivos.
6. Controlar y verificar las autorizaciones de la emisión de comprobantes de pago, incluyendo los trabajos que realizan las imprentas.
7. Disminuir el porcentaje de omisos a la presentación.
8. Contar oportunamente con la información de Red Bancaria, para que pueda se utilizada en el control y cobranza de la deuda.
9. Determinar la deuda tributaria de los medianos y pequeños contribuyentes.
10. Disminuir la deuda sin pagar a través de la optimización de las acciones de cobranza coactiva.
11. Mejorar el servicio bancario de atención a los contribuyentes.
12. Mejorar la calidad de la información de gestión a fin de optimizar la toma de decisiones.

1.3.2 SISTEMAS DE FISCALIZACIÓN

1. Incrementar el riesgo entre los principales y medianos contribuyentes, mediante acciones de fiscalización de carácter masivo y de mayor profundidad.

2. Profundizar las auditorías realizadas en los casos de presunción de delito tributario, con criterio selectivo.
3. Mejorar la calidad de los programas de fiscalización:
   a. Métodos de Selección
   b. Oportunidad en la Programación
4. Mejorar la calidad de los valores que se emiten.
5. Resolver en el menor tiempo posible las solicitudes de devolución de impuestos. evitando la acumulación de expedientes sin resolver.
6. Mejorar la calidad en la resolución de expedientes no contenciosos.
7. Mejorar la difusión de las instrucciones de nivel normativo en los aspectos legales, reglamentarios y de procedimientos.
8. Desarrollar y mejorar la calidad de los procedimientos de auditoría.
9. Racionalizar la información requerida para control de gestión.
10. Interiorizar a los auditores los conceptos y fundamentos de hechos y de derecho contenido en las resoluciones que emite el área de reclamaciones.

1.3.3 RESOLUCIÓN DE RECLAMOS

1. Resolver con uniformidad y equidad, en el menor tiempo posible los recursos de reclamación evitando la acumulación de expedientes sin resolver.
2. Mejorar la calidad en la resolución de expedientes.

1.3.4 ATENCIÓN AL CONTRIBUYENTE

1. Consolidar la política de Atención al Contribuyente a nivel nacional.
2. Desarrollar y descentralizar los Sistemas de Atención al Contribuyente a nivel nacional.
3. Organizar programas de difusión masiva de las Normas Tributarias.

1.3.5 DIFUSIÓN Y EDUCACIÓN DEL CONTRIBUYENTE

1. Desarrollar el proyecto de Educación en la Escuela en convenio con el Ministerio de Educación.
2. Elaborar y distribuir material de difusión (cuadernillos, folletos, trípticos) sobre los aspectos más importantes de las normas y procedimientos tributarios.
3. Apoyar en la realización de las jornadas de SUNATHON, en lo concerniente a la atención y orientación al público asistente.

CAPITULO II : MARCO TEÓRICO

2.1 DEFINICIÓN DE AUDITORÍA DE SISTEMAS

La palabra auditoría proviene del ingles "to audit", el cual significa verificar, inspeccionar. Asimismo, el término inglés "audit" encuentra su origen en las voces latinas "audire"(oir), "auditio"(acto de oír o audición de una lectura pública o de una declamación) o "auditus" (oído, facultad de oír).

En el sentido amplio se puede definir a la auditoría como un examen critico, que va a permitir verificar el sistema de información y su funcionamiento, con el objeto de determinar la confiabilidad de la información que produce, corregir los errores y proponer alternativas de solución. Dicho examen también nos va a permitir evaluar la eficiencia y eficacia de las operaciones.

Entonces se puede definir a la Auditoría de Sistemas como

> "Examen que se realiza en un ambiente que cuenta con procesamiento electrónico de datos y que las características de este ambiente se deben adecuar los procedimientos, las técnicas y las herramientas tradicionales de auditoría a los cambios substanciales que presenta el computador al desarrollar los sistemas de información de la entidad".[1]

Auditoría de Sistemas de Información
IBM del Perú

2.2 CONCEPTOS DE AUDITORIA

Estos conceptos son una guía para el proceso de auditoría, a fin de lograr un entendimiento de la estructura de control interna, establecer un control de riesgos y diseño de las pruebas sustantivas.

Muchas veces para optimizar el tiempo del auditor se realizàn concurrentemente las pruebas de control y las pruebas sustantivas. Esto se conoce como Pruebas de Propósito Dual, el cual es aplicable en todo tipo de auditorías.

2.2.1 ENTENDIMIENTO DE LA ESTRUCTURA DE CONTROL INTERNA

Esta parte del proceso sistemático de la auditoría es necesaria para realizar la planificación de la misma, a fin de determinar que controles han prescrito. El entendimiento de la estructura de control interno, provee las bases preliminares para establecer un primer nivel de control de riesgos, los cuales van a enriquecerse conforme avanza el proceso de auditoría.

Requiere del entendimiento de tres elementos:

El control del ambiente,

El accounting del sistema, y

El control de los procedimientos.

Los objetivos del entendimiento de la estructura de control interno son:

a) Identificar los errores potenciales,

b) Considerar los factores riesgos, y

c) Diseñar las pruebas sustantivas.

2.2.2 ESTABLECER UN CONTROL DE LOS RIESGOS

El propósito de establecer un control de los riesgos es evaluar la eficiencia de las políticas y procedimientos de la estructura de control interno a fin de prevenir o detectar errores. Representa un nivel intermedio entre los procedimientos de evaluación del control interno y las pruebas sustantivas.

Para determinar si los controles establecidos dentro del computador funcionan apropiadamente, es necesario utilizar técnicas computarizadas. Las pistas de auditoría, es usada por los auditores para realizar un seguimiento de las transacciones. Adicionalmente, se utilizan otros controles como los controles generales y los controles de aplicación, los cuales son discutidos posteriormente.

El auditor debe establecer el control de riesgos en dos áreas:

a) Establecer el control en todas las aplicaciones vitales.
b) Establecer un control entre el Departamento de Procesamiento de la Información y las áreas usuarias.

El auditor también debe considerar establecer controles de usuarios, debido a que pueden resultar más efectivos que los controles generales y controles de aplicación, dando como resultado una mixtura de controles que nos permiten establecer un sistema completo de control de riesgos.

2.2.3 DISEÑAR LAS PRUEBAS SUSTANTIVAS

Después del establecimiento del control de riesgos, el auditor debe recolectar evidencia competente que sustente el informe de auditoría, con el propósito de determinar si el computador esta procesando apropiadamente las transacciones.

Las pruebas sustantivas tiene dos componentes relevantes:

a) **Pruebas de detalles de Transacciones y Balances**

El alcance de éstas pruebas difiere dependiendo del nivel tecnológico de los sistemas. En aquellos computadores con un nivel tecnológico simple, las pruebas serán parecidas a las realizadas con un sistema manual. Sin embargo, en aquellos computadores con un nivel de complejidad alto, es necesario utilizar computadores y software de auditoría especializado para poder obtener las pruebas sustantivas.

b) **Procedimientos Analíticos**

Permiten detectar errores o irregularidades del procesamiento de la información, analizando y comparando la información histórica.

2.2.4 ROL DEL AUDITOR DE SISTEMAS Y LA COMPUTADORAS EN EL FUNCIONAMIENTO DE LAS PRUEBAS DE CONTROL Y LAS PRUEBAS SUSTANTIVAS

Aquí se define como el Auditor de Sistemas usa el computador para asegurar los procedimientos cuando estas pruebas están funcionando. Para ello es necesario que el auditor seleccione las técnicas apropiadas que le permitan realizar el proceso de auditoría.

Al realizar el proceso de auditoría, se le presenta al Auditor de Sistemas tres fases: Auditoría Alrededor del Computador[2], Auditoría a través del Computador[3] y Auditoria con el Computador[4]. El auditor de sistemas debe escoger un caso particular o una combinación de ellos, dependiendo del alcance de la auditoría.

[2] La Auditoría alrededor del Computador, se realiza sin utilizar el computador. Generalmente, comprende la Evaluación de los Controles Generales y la Revisión de Seguridad

[3] La Auditoría a través del Computador, enfoca al computador y los programas, examinando los resultados del procesamiento de la información. Comprende la Evaluación de los Controles de Aplicación.

[4] La Auditoría con el Computador, utiliza el computador y programas como una herramienta de auditoría.

El Auditor de Sistemas debe saber en que parte del ciclo de procesamiento aplicar las técnicas de auditoría : cuando el computador esta procesando o después que ha terminado el procesamiento. En el primer caso es necesario determinar el momento oportuno para obtener la información, el cual puede ser diseñado en los sistemas o se puede obtener mediante queries.

Adicionalmente, el Auditor de Sistemas debe determinar donde colocar las técnicas de auditoría: en la fases de procesamiento o en los resultados. Auditar las fases del procesamiento, se refiere al establecimiento del control de riesgos, donde está incluido la evaluación de los controles generales y de los controles de aplicación. Auditar los resultados del procesamiento se refiere primordialmente a la recolección de evidencia.

El Auditor de Sistemas debe determinar que auditar: programas, archivos o el sistema entero. Para ello se puede aplicar las técnicas de auditoría con ayuda del computador (CAAT [5]), dependiendo de los objetivos de auditoría, los cuales a su vez determinan si se utilizan procedimientos de auditoría individuales de programas y archivos o se utilizan procedimientos de auditoría del sistema entero como un todo integrado.

2.3 PLANIFICACIÓN DE LA AUDITORIA

La planificación de la auditoría es el primer paso que debe realizar el Auditor de Sistemas, a fin de comprender el ambiente donde se va a realizar la auditoría, así como riesgos y controles inherentes al mismo.

---

5 CAAT : Computer Assisted Auditing Techniques

2.3.1 COMPRENSIÓN GLOBAL DEL NEGOCIO

Es necesario que el Auditor de Sistemas comprenda como funciona el ambiente que se esta revisando, el cual debe incluir el tipo de información que utilizan, las prácticas comerciales y funciones relacionadas con la auditoría, así como comprender el ambiente normativo en que opera el negocio.

2.3.2 EVALUACIÓN DEL RIESGO

El Auditor de Sistemas debe tener una cabal comprensión de los riesgos al Planificar la Auditoría, con el propósito de asegurar la continuidad del negocio, considerando que riesgo es cualquier evento no deseado.

El auditor debe realizar una evaluación de las áreas funcionales del negocio a fin de determinar las áreas de alto riesgo que deben ser auditadas[6]. Para ello es necesario crear un grupo de Análisis de Riesgos, el cual debe determinar:

- Los riesgos a los que están sujetos la información y su impacto financiero en la empresa.
- Medidas que se pueden adoptar para reducir la ocurrencia y el impacto de los riesgos, y su costo.
- Las medidas que deben ser adoptadas en base al análisis de costo beneficio.

2.3.3 ÁREAS DE LA AUDITORIA Y PROCEDIMIENTOS DE CONTROL DE SISTEMAS DE INFORMACIÓN

Luego de realizar el análisis de riesgos, se puede agrupar a las auditorías en los siguientes áreas:

---

6 Metodología de Análisis de Riesgos se describe en el Anexo 1

a) Revisión de los controles generales : Estructura Organizativa Gerencial, políticas, procedimientos operativos y ambiente de control del Sistema de Información.

b) Revisión de Centros de Cómputo Operaciones de las instalaciones de procesamiento de información.

c) Revisión de Seguridad : Acceso lógico, acceso fisico y controles del ambiente.

d) Recuperación en Desastres : Políticas y procedimientos referentes a la planificación de los desastres.

e) Sistema Operativo : Políticas y procedimientos de desarrollo, adquisición y mantenimiento de software de sistemas operativos.

f) Revisión del ciclo de vida del desarrollo de sistemas : Metodología, normas, tareas y procedimiento para el desarrollo, mantenimiento y adquisición de software.

g) Revisión de control de Aplicaciones : Evaluar y analizar las fortalezas y debilidades de control y operaciones de los sistemas aplicativos existentes.

Los procedimientos de control de Sistemas de Información están relacionados con las áreas de auditoría, tal como se muestra en la siguiente clasificación :

- Políticas y procedimientos de seguridad lógica de la organización para garantizar la adecuada autorización de transacciones y actividades.
- Políticas globales para el diseño y utilización de documentos y registro auditables de transacciones (rastros de auditoría).
- Procedimientos y funciones a fin de evitar acceso no autorizado a los activos e instalaciones.
- Políticas de seguridad fisica de los centros de cómputo.
- Procedimientos de Control de Organización General

- Acceso a datos y programas
- Metodologías de desarrollo de sistemas
- Operaciones de procesamiento de datos
- Funciones de programación de sistemas y Soporte Técnico
- Procedimientos de control de calidad de procesamiento de datos

2.3.4 DESARROLLO DEL PROGRAMA DE AUDITORIA

Aunque un programa de auditoría no se guía por un conjunto de pasos determinados, es necesario seguir pasos secuenciales para lograr una comprensión del ente auditado.

Un programa de auditoría es un conjunto de procedimientos de auditoría, diseñados para lograr los objetivos de auditoría. Asimismo, el programa de auditoría se convierte en una guía de documentación de los diversos pasos de auditoría.

Un programa de auditoría incluye lo siguiente:

- *Tema de Auditoría*
- *Objetivo de Auditoría*
- *Alcance de Auditoría*, identificando temas o unidades organizacionales que comprende la auditoría.
- *Planificación previa a la auditoría*
  - Identificar recursos con que se cuenta
  - Identificación de fuentes de información
  - Identificar lugares físicos o instalaciones a auditar
- *Procedimientos de Auditoría*
  - Recopilación de Datos

- Identificación del enfoque de auditoría para verificar y probar controles.
- Listas de personas a ser entrevistadas
- Obtener copia de las normas, políticas y directivas
- Desarrollo de herramientas y metodología de auditoría para probar y verificar controles.

- *Procedimientos para evaluar los resultados de las pruebas*
- *Preparación de Informe de Auditoría*
- *Procedimientos de Seguimiento*

Un programa de auditoría no es eficaz, si no se han tomado las acciones correctivas según las recomendaciones de auditoría y además, si no se realiza un seguimiento a dichas recomendaciones. Es por ello, que generalmente se dice que la auditoría es un proceso continuo.

2.4 AUDITORIA DE LOS CONTROLES DE ORGANIZACIÓN Y ADMINISTRACIÓN

El uso del computador en el procesamiento de la información frecuentemente elimina los controles establecidos, utilizándose controles alternativos que permitan compensarlos.

El objetivo de los Controles de Organización y Administración es examinar la existencia de controles en todas las áreas donde se procesan información, a fin de recomendar la incorporación de normas y procedimientos en aquellas áreas que representen un riesgo para la organización.

2.4.1 POLÍTICAS, ESTÁNDARES Y PROCEDIMIENTOS

Es necesario comprobar que las directivas emitidas por la alta dirección hayan sido comunicados oportunamente a las áreas involucradas, con el propósito de verificar su adecuada utilización.

Los estándares deben ser revisados a fin de entender el proceso mediante el cual se desarrollan, aprueban, distribuyen y actualizan los mismos. Esto a su vez permite evaluar el nivel de cumplimiento de los departamentos usuarios y del Departamento de Informática.

Los procedimientos estándares de operación, permiten el uso de técnicas uniformes, los cuales aumentan la probabilidad de un procesamiento de calidad y ayudan a proteger los archivos y programas de pérdida, destrucción, manipulación o acceso no autorizado.

Finalmente, es necesario revisar los procedimientos de operación relativos a las responsabilidades de funcionamiento, entre los departamentos usuarios y el Departamento de Informática.

2.4.2 RESPONSABILIDADES ORGANIZACIONALES

El Departamento de Informática es un área importante dentro de la jerarquía organizacional, debido a que contribuye al logro de los objetivos de las áreas usuarias, es por ello la necesidad de ubicarlo en un nivel alto dentro de la estructura organizacional a fin de mantener su independencia de los departamentos usuarios.

Asimismo, es necesario revisar las principales unidades organizacionales que conforman el Departamento de Informática, con sus responsabilidades delineadas y documentadas. Debe existir una adecuada separación de tareas dentro este departamento, a fin de dividir las responsabilidades del manejo de errores, los cuales están basadas en la separación de las cuatro funciones básicas de

autorización, ejecución y registro de transacciones, y el mantenimiento del accountability de todas éstas transacciones.

La segregación de tareas no elimina completamente el riesgo, pero sin embargo aumenta la dificultad para identificar cambios en los sistemas o programas de aplicación con el propósito de cometer un error deliberado, debido a que es necesario conocer tanto los sistemas, como la operación de los mismos.

2.4.3 CONTROL DE CALIDAD DE LOS SISTEMAS DE INFORMACIÓN

Con el propósito de garantizar la calidad de los servicios proporcionados por los sistemas de información a los departamentos usuarios, se deben establecer medidas formales mediante una función de control de calidad de los sistemas de información.

El grado de satisfacción de los usuarios debe ser evaluada, en lo que se refiere a los servicios proporcionados por el Departamento de Informática. Además se debe verificar si se han atendido las necesidades de software (de aplicación y de operación) y hardware de los departamentos usuarios.

Asimismo, se debe incluir una revisión de la forma en que los sistemas y las aplicaciones han contribuido al logro de los objetivos de los sistemas de información de la organización.

2.5 REVISIÓN DEL CICLO DE VIDA DEL DESARROLLO DE SISTEMAS

Las empresas generalmente invierten una considerable cantidad de recursos humanos y gastos en efectivo para el desarrollo, adquisición o mantenimiento de un sistema. Es por ello que el Auditor de Sistemas debe comprender la metodología de desarrollo o

adquisición de sistemas a fin de poder determinar los puntos débiles que exijan un control.

2.5.1 CONTROLES DEL CICLO DE DESARROLLO DE SISTEMAS

Debe existir una adecuada y completa documentación de cada una de las etapas del Ciclo de Desarrollo de Sistemas, el cual considere por los menos lo siguiente:

a) Objetivos a lograr en cada una de las fases
b) Producto final que debe ser entregado en cada una de las fases
c) Cronograma de proyecto, señalando la fecha de entrega de cada uno de los productos finales.
d) Aprobación del Jefe de Proyecto y de los Usuarios

La revisión de calidad es necesario, con el propósito de determinar si el sistema cumple con los requerimientos del negocio. Las desviaciones de los requerimientos es el primer y más devastador riesgo potencial, debido a que no cumple con las necesidades y expectativas de los usuarios, motivo por el cual deben ser identificadas lo más rápido posible.

Al auditor de sistemas debe tener una participación activa en el desarrollo del proyecto, con el propósito de implementar los controles adecuados, debido a que existe un mayor grado de dificultad para implantar controles cuando el sistema ya este construido. Un riesgo mayor, es que la falta de controles no es detectada por un largo periodo de tiempo, en el cual puedan ocurrir actividades fraudulentas.

Asimismo, el diseño del sistema debe contemplar políticas de seguridad que permitan proteger programas, transacciones y bases de datos. El diseño debe

incluir funciones para generar y mantener pistas de auditoría, que permitan la auditabilidad[7] de las transacciones.

2.5.2 AUDITORÍA PARA LA ADQUISICIÓN DE SOFTWARE

Para la adquisición de software es necesario iniciar un proceso de evaluación del producto y de proveedor que lo comercializa, utilizando los siguientes criterios:

1. Viabilidad del Vendedor : El vendedor del producto debe tener una buena reputación, así como también una sólida situación financiera. Se tiene que tener especial cuidado con los vendedores de productos nuevos, especialmente si el comprador es el primer cliente de dicho producto.
2. El vendedor debe estar en condiciones de proveer una documentación completa y confiable del sistema para su evaluación antes de realizar la adquisición del software.
3. Soporte del vendedor, es decir, contar con una línea completa de productos de respaldo, incluyendo consultas telefónicas, entrenamiento a los usuarios durante la implantación, upgrades del software, etc.
4. Disponibilidad del código fuente en caso de que el sistema sea desarrollado a medida, estableciendo cláusulas que incluyan la actualización del software.
5. Evaluar la performance del software en otras empresas, así como el tipo de tecnología utilizada en su desarrollo, a fin de evitar que el software se convierta obsoleto en poco tiempo.

Para la adquisición de software es necesario crear un equipo de evaluación, el cual debe incluir a personal técnico especializado, así como a usuarios claves, los cuales van a determinar cual es el producto que ofrece la mejor solución al mejor precio. Es necesario revisar la documentación relacionada a los proveedores, el cual debe incluir:

---

[7] Auditabilidad es la facultad con que una transacción puede ser seguridad a través del sistema.

- Estabilidad Financiera
- Número de años de experiencia ofreciendo el software
- Números de clientes que usan el software
- Compromiso de servicio
- Compromiso de desarrollar o mejorar el software
- Nivel de Satisfacción de otros clientes
- Dirección tecnológica y capacidad de los vendedores de dar soporte.
- Compromiso de entrenamiento, documentación o upgrades del software.
- Aceptación de pruebas del software antes de comprarlo.

Asimismo, es necesario tener en cuenta lo siguiente al realizar una revisión de los contratos:

- Descripción específica de software a entregar
- Compromiso de entrega del software
- Compromiso de entrega de documentación, entrenamiento y upgrades del software
- Acuerdo de mantenimiento y entrega de las licencias de uso respectivas.

2.5.3 AUDITORÍA DEL DESARROLLO DE APLICACIONES

Muchas aplicaciones son desarrolladas sin tener en cuenta metodologías adecuadas de desarrollo y documentación de los sistemas, obligando al Auditor de Sistemas a establecer controles a fin de que una aplicación funcione de acuerdo a las especificaciones.

"El propósito de los controles de desarrollo y documentación de los sistemas es crear un ambiente que asegure al auditor que los controles de aplicación

están incluidos en todos los sistemas y que la integridad de los mismos se mantienen aún después de haber sido implantados"[8]

Durante todo el ciclo de desarrollo de sistemas el auditor debe analizar los riesgos y los expuestos que son inherentes a cada una de las fases, a fin de asegurar que los mecanismos de control están vigentes y minimizar los riesgos. Es menos costoso establecer controles desde el inicio del Ciclo de Desarrollo de Sistemas en vez de colocarlos al final de este ciclo, es por ello que algunas empresas incluyen la participación de un Auditor de Sistemas en el desarrollo de sistemas a fin de asegurar que los sistemas trabajen apropiadamente e incluir adecuados controles de aplicación. Asimismo, es necesario realizar una revisión posterior a la implantación del sistema a cargo de un auditor independiente al que participó en el Ciclo de Desarrollo de Sistemas.

La labor del Auditor de Sistemas consiste en:

1. Determinar los objetivos y requerimientos de los usuarios de los sistemas e identificar las áreas que exigen controles.
2. Determinar y clasificar los principales riesgos y expuestos del sistema con el propósito de implementar controles.
3. Identificar los controles para minimizar riesgos y expuestos .
4. Asesorar el equipo de proyecto en el diseño e implantación de controles dentro de los sistemas.
5. Monitorear el proceso de desarrollo de sistemas para asegurar de que se implantan controles, se cumplen los requerimientos de los usuarios, se sigue una metodología de desarrollo de sistemas y que el sistema es eficaz y eficiente.

---

[8] Tomado de Auditing EDP Systems

6. Coordinar la revisión post-implantación.

El Auditor de Sistemas debe obtener la documentación necesaria y disponible de cada una de las fases de desarrollo de sistemas, brindando asesoramiento al equipo de desarrollo durante todo el proceso. Asimismo, se debe evaluar la capacidad de los equipos del proyecto de entregar los avances en cada una de las fechas establecidas.

El control del Desarrollo de Sistemas empieza estableciendo procedimientos estándares para la planificación, desarrollo e implantación de los sistemas; es decir se necesita de una Metodología de Desarrollo de Sistemas.

2.5.3.1 ESTUDIO DE FACTIBILIDAD

El Auditor de Sistemas debe revisar toda la documentación producida de esta fase, a fin de analizar la relación de costo/beneficio que justifique el desarrollo del sistema y especialmente para determinar hasta que punto existe la necesidad del software, es decir si es técnica, operacional y económicamente factible.

En esta fase es necesario determinar si se puede obtener una solución con los sistemas ya desarrollados o evaluar las soluciones alternativas y si se eligió la solución más apropiada.

2.5.3.2 DEFINICIÓN DE REQUERIMIENTOS

El Auditor de Sistemas debe obtener documentación detallada de esta fase, verificando su exactitud por medio de entrevistas con los usuarios de las unidades organizacionales involucradas, lo cual a su vez va a permitir determinar el grado de participación de los usuarios.

En esta fase es necesario revisar los diagramas de flujo y el diseño conceptual para asegurar de que se tratan de los requerimientos de los usuarios y que además se han considerado niveles de control apropiados y que la aplicación es auditable.

2.5.3.3 DISEÑO DETALLADO Y PROGRAMACIÓN

En esta etapa es necesario revisar los flujogramas del sistema para lograr una comprensión general del diseño general. En caso de observarse cambios al diseño general , en necesario verificar que dichos cambios cuenten con las autorizaciones apropiadas del Jefe de Proyecto y de los Usuarios.

Las tareas a realizar por el Auditor de Sistemas son:

- Revisar que los controles de entrada/salida diseñados sean apropiados.
- Verificar que los cálculos se realicen correctamente, así como los procesos claves.
- Verificar que el sistema puede identificar y procesar correctamente datos erróneos.
- Verificar que las pistas de auditoría recomendados o módulos de auditoría fueron incorporados, a fin de permitir la auditabilidad del sistema, y así poder rastrear la información clave.
- Verificar que se utilicen los estándares de programación.

2.5.3.4 FASE DE PRUEBA

Esta fase es muy importante, por que es la última oportunidad antes de la implementación de descubrir y corregir los problemas, y es aquí donde se determina si los requerimientos han sido satisfechos, siendo la participación del Auditor de Sistemas intensiva al revisar esta fase. El propósito de las pruebas del sistema es:

- Asegurar que el sistema funciona de acuerdo a las especificaciones del diseño.
- Determinar si la operación del sistema cubre todos los requerimientos de los usuarios.
- Probar que los controles de aplicación funcionan tal como fueron diseñados.

Las pruebas de los sistemas es un esfuerzo conjunto de los usuarios, personal de sistemas y los auditores internos o externos, el cual puede tener 5 niveles diferentes de profundidad: Pruebas de Programas, Pruebas de Procesos (String Tests), Pruebas del Sistema, Pruebas Pilotos y Pruebas Paralelas.

2.5.3.5 IMPLANTACIÓN

El Auditor de Sistemas debe verificar de que se han realizado las aprobaciones necesarias antes de transferir un nuevo sistema a situación de producción. Este control permite examinar los resultados de las pruebas finales, con el propósito de conocer la eficiencia de los controles de aplicación y asegurar que todos los errores han sido corregidos. Es necesario revisar la documentación a fin de asegurarse de que esta completo y que todas las actualizaciones de la Fase de Prueba están incorporadas.

En esta fase se verifica el proceso de conversión de datos para asegurarse de que es exacta y esta completa antes de realizar la implantación del sistema. Esta fase no es completada hasta resolverse todas la incompatibilidades entre el antiguo sistema y el nuevo.

2.5.3.6 POST-IMPLANTACION

En esta fase es necesario que el Auditor de Sistemas sea independiente a las otras fases del desarrollo del sistema, a fin de mantener la objetividad. El sistema debe estar en producción por lo menos durante seis (6) meses, con el propósito de que aparezcan todos los problemas significativos.

El significado de la revisión post-implementación para los auditores es proporcionar una retroalimentación a fin de determinar que controles están funcionando eficientemente y que controles necesitan implementarse. Es una buena oportunidad para realizar ajustes que serían implementados en el futuro.

Las tareas a realizar por el Auditor de Sistemas son:

- Considerar la utilización del sistema y la satisfacción de los usuarios finales, debido a que ellos constituyen un indicador de que el sistema ha cumplido con los requerimientos de los usuarios, y además permiten medir adecuadamente los beneficios los beneficios identificados en el estudio de factibilidad.
- Revisar las solicitudes de cambios a los programas para evaluar los tipos de cambios que se exigen al sistema, el cual puede indicar problemas en el diseño, programación o interpretación de los requerimientos de los usuarios.
- Revisar los controles para asegurarse de que operan de acuerdo al diseño y si el módulo de auditoría ha sido incorporado al sistema.
- Revisar los logs de error del operador para verificar si existen problemas de recursos u operaciones que son inherentes al sistema.

- Revisar los saldos de control de entrada/salida para verificar que el sistema esta procesando los datos de manera exacta y correcta.

2.5.4 CONTROL SOBRE CAMBIOS A PROGRAMAS

El control sobre cambios a programas se refiere a proceso de mover programas del entorno de pruebas al entorno de producción. Un sistema desarrollado, probado y puesto en funcionamiento pocas veces permanece estático, siendo necesario realizar y registrar todos los cambios. Sin un adecuado control sobre las modificaciones de los programas, la integridad de los sistemas puede ser destruida.

La tarea del Auditor de Sistemas es asegurar que existe un adecuado control sobre los cambios a los programas. Los objetivos del control de cambios a los programas son para asegurar que todos los cambios han sido aprobados y autorizados, y para asegurar que todas las autorizaciones son completas, probadas y apropiadamente implementadas.

Las tareas a realizar por el Auditor de Sistemas son:

- Evaluar los estándares y procedimiento de cambios a programas en producción, verificando la aceptación y autorización del usuario.
- Probar los procedimientos de control de cambios para asegurar que se aplican según los estándares establecidos.
- Evaluar el proceso de control de los cambios, así como verificar que exista un rastro de auditoría de los mismos, tales como : ID del programador, fecha y hora del cambio, número de solicitud asociada con el cambio.
- Verificar que la documentación de los sistemas se encuentre actualizada, a fin de permitir el mantenimiento oportuno y continuo del sistema.

2.5.5 ESTÁNDARES DE DOCUMENTACIÓN DE LOS SISTEMAS

El auditor debe enfatizar la importancia de establecer normas adecuadas de documentación, la misma que es útil para múltiples propósitos, brindando un punto de partida para lograr el entendimiento de las aplicaciones. Adicionalmente, es una herramienta para planear y supervisar la implantación de nuevas aplicaciones en el computador.

Una buena documentación es importante para el diseño e implantación de un sistema bien controlado y sirve como una fuente de información. Si no se establecen normas adecuadas de documentación el Auditor de Sistemas debe buscar otras fuentes de información, la cual puede ser difícil de obtener y aumenta el costo de las tareas que debe realizar. Generalmente la documentación permite:

1. Entender los objetivos y conceptos del sistema y de los resultados que produce.
2. Brindar información para los analista de sistemas y programadores que son responsables de mantener y revisar los programas y sistemas actuales.
3. Capacitar al personal nuevo y fuente de información que es indispensable para proporcionar continuidad en el caso de retiro de personal experimentado.
4. Servir de medio de información común a otros analistas de sistemas, programadores y operadores.

La preparación de la documentación demanda una apreciable cantidad de tiempo y esfuerzo. Debe estar sujeta a un estricto control y revisión , para lograr un desarrollo adecuado. Para que la documentación sea efectiva, debe ser completa y haber sido preparada de conformidad con una norma determinada previamente, que debe establecerse antes del inicio del diseño de los sistemas y la programación.

2.5.5.1 DOCUMENTACIÓN SOBRE DEFINICIÓN DEL PROBLEMA

Al revisar esta documentación, el auditor estará en capacidad de obtener un entendimiento general del sistema sin involucrase en los detalles de los programas. Esta documentación debe incluir:

- Descripciones de las razones para implantar el sistema
- Descripción de las operaciones ejecutadas por el sistema
- Inclusión de las propuestas para el proyecto
- Suministro de evidencia de aprobación del sistema y cambios posteriores
- Lista de la asignación de responsabilidades en el proyecto

2.5.5.2 DOCUMENTACIÓN DE LOS SISTEMAS

La documentación de los sistemas proporciona suficiente información para rastrear los datos de entrada hasta llegar al producto final del sistema. El auditor esta en capacidad de determinar si existe un rastro adecuado para la auditoría. Asimismo, es posible determinar que datos no están impresos pero son de utilidad para el desarrollo de la auditoría. La documentación de sistemas incluye:

- Descripción de los sistemas;
- Flujogramas de los sistemas mostrando el flujo de datos a través del sistema y la interrelación entre los pasos del proceso y las rutinas del computador
- Descripciones de la entrada
- Descripciones de la salida
- Descripciones de archivos
- Descripciones de controles

- Copias de las autorizaciones y las fechas en que se hayan efectuado cambios en los sistemas ya implantados.

2.5.5.3 DOCUMENTACIÓN DE LOS PROGRAMAS

Mientras que la documentación de los sistemas el trabajo del sistema completo, la documentación de los programas enfoca el detalle de la información de cada programa en el sistema. Este detalle permite mantener un control sobre los cambios a los programas, definiendo el estado actual de cada programa. La documentación de cada programa incluye lo siguiente:

- Una breve descripción del programa
- Flujograma, tabla de decisiones o descripción detallada de como opera cada programa
- Lista de controles
- Descripción detallada del formato de los archivos y los planos de los registros
- Tabla de los valores de los códigos utilizados para indicar los requisitos de proceso
- Registro de cambios a los programas, sus autorizaciones y la fecha efectiva de tales autorizaciones
- Formatos para entrada y salida
- Instrucciones de operación
- Descripción de las características especiales de control tales como rutinas para la detección de errores y el uso de tablas.

2.5.5.4 DOCUMENTACIÓN DE LAS OPERACIONES

La documentación de las operaciones puede revisarse para tener un conocimiento de las funciones ejecutadas por el grupo de operaciones y para determinar como se procesa la información dentro del Departamento de

Sistemas. La información que se debe suministrar al operador incluye lo siguiente:

- Breve descripción del proceso
- Descripción de los requisitos de entrada y salida (formas y formatos utilizados)
- Secuencia de discos, cintas y archivos
- Indicación de los mensajes al operador, altos y la acción que debe seguirse para finalizar trabajos
- Procedimientos de control que debe ejecutar las operaciones
- Procedimientos de recuperación y reiniciación que se utilizan cuando hay mal funcionamiento de los equipos y los programas
- Estimados de tiempos normal y máximo por cada rutina
- Instrucciones al operador en caso de emergencia.

2.5.5.5 DOCUMENTACIÓN DEL USUARIO

Los departamentos usuarios que reciben servicios del Departamento de Sistemas, deben contar con una descripción de las instrucciones de usuarios, las cuales deben incluir los requerimientos de entrada, salida y procedimientos para el manejo de errores. La documentación del usuario debe revisarse para conocer las funciones que éste ejecuta y para determinar el flujo de información entre el usuario y el Departamento de Sistemas.

La documentación de usuario es valiosa para el auditor con el propósito de entender el rol del usuario en el procesamiento de la información y en la evaluación del grado de control provista por el usuario. La documentación del usuario comúnmente incluye lo siguiente:

Descripción no técnica de como funciona el sistema, incluyendo los beneficios que el usuario obtendrá del sistema.

- Descripción de los documentos de entrada entradas, así como una descripción de los reportes de salida.
- Lista de procedimientos de control con una indicación de la persona responsable de ejecutar dichos procedimientos. Esta responsabilidad se identifica por la posición y no por el nombre de la persona
- Procedimientos para la corrección de errores en el ingreso de la data o en el procesamiento de la misma
- Procedimientos para envío de datos al Departamento de Sistemas, incluyendo días y horas para el envío de la información.
- Descripción del procedimiento que deben emplear los usuarios para verificar la exactitud de los informes.

2.6 PROCESO DE AUDITORIA A LOS CONTROLES DE APLICACIÓN

Este proceso permite asegurar que los Controles de Aplicación de entrada, procesamiento y salida están correctamente diseñados. Estos controles incluyen métodos que aseguren que sólo se ingresan y actualizan datos exactos, completos y válidos; es decir, el procesamiento realiza la tarea correcta; los resultados del procesamiento cumplen con los requerimientos; y se mantiene la integridad de la información.

2.6.1 PROCEDIMIENTOS DE CONTROL DE ENTRADA

Estos procedimientos controlan el ingreso de transacciones directamente al computador por medio de un terminal. Permiten asegurar que cada transacción es recibida, procesada y registrada de manera exacta y en su totalidad, además de asegurar que sólo se procesan transacciones debidamente autorizadas.

2.6.1.1 PROCESO DE AUTORIZACIÓN DEL INGRESO

El Auditor de Sistemas debe verificar que todas las transacciones han sido debidamente autorizadas. Se debe verificar las siguientes autorizaciones:

- La correcta autorización en la firma de los formularios de encabezamiento de lotes.
- Controles de acceso on-line, a fin de asegurar que solo personas autorizadas tiene acceso a los datos.
- Passwords exclusivos con el propósitos de identificar al responsable en el caso de cambio a los datos.
- Control adecuado de los documentos fuentes, verificando que estén correctamente prenumerados, a fin de poder controlar el ingreso de los mismos.

2.6.1.2 PROCESO DE VALIDACIÓN Y EDICIÓN DE DATOS

Se identifica errores e incongruencias en los datos, utilizándose para ello los siguientes tipos:

- Control de Secuencia, permite verificar si el número de control sigue la secuencia correcta.
- Control de Límite, los datos no deben pasar una cantidad determinada.
- Control de Rangos, los datos deben estar por un rango determinado.
- Control de Validez y Existencia, controles programados de la validez de los datos de acuerdo con criterios predeterminados.
- Control de Razonabilidad, los datos ingresados se comparan con límites de razonabilidad.
- Búsqueda en Tablas, verifica los datos ingresados con criterios establecidos en una tabla.
- Doble Verificación del Ingreso, el ingreso es repetido por otra persona, a fin de concordar la digitación original con la reingresada.
- Dígito de Control, se adiciona un valor numérico, el cual es calculado matemáticamente.

- Control de Integridad, un campo siempre debe contener datos y no ceros o blancos.
- Control de Duplicación, se chequean las transacciones con las ya ingresadas, con la finalidad de que no hayan sido ingresadas anteriormente.

2.6.1.3 CONTROLES POR LOTE Y DE BALANCEO

Los controles de lotes agrupan manualmente transacciones de ingreso con el propósito de obtener totales de control. El control de lote puede basarse:

- Total de Montos
- Total de Items
- Total de Documentos

Los Balanceos de Lotes permiten asegurar que cada transacción crea un documento de entrada, que todos los documentos se incluyen en un lote, que se presentan todos los lotes para su procesamiento, que todos los lotes son aceptados por el computador, que se realiza la conciliación de la totalización del lote, que existen procedimientos para la investigación y oportuna corrección de las diferencias, y que hay controles respecto de la nueva presentación de las transacciones rechazadas.

Existen diversos tipos de balanceos:

- Registros de Lotes
- Cuentas de Control, determinando manualmente los totales de lotes para luego conciliarlos con los totales procesados.
- Concordancia Computarizada, por medio de formularios de encabezamiento de lote que registran el total del lote.

2.6.2 PROCEDIMIENTOS PARA EL CONTROL DEL PROCESAMIENTO

El procesamiento es una función interna del computador que consiste en ejecutar operaciones sobre data, de acuerdo con instrucciones de programas. Las operaciones durante el procesamientos incluye validación de data, cálculos, comparaciones, actualización de archivos, mantenimiento de archivos, correcciones de errores, y muchas otras funciones más.

Los controles de procesamiento son importantes para la detección de errores. Sin embargo, los programas de aplicación son frecuentemente actualizados, corregidos o implantados sin un adecuado control, utilizando frecuentemente una versión incorrecta. Es por ello la necesidad de utilizar controles que aseguren la utilización correcta de las versiones.

Los archivos de datos son también cambiados como resultado del procesamiento de transacciones y del mantenimiento de archivos, siendo necesario realizar un control de librerías, procedimientos estándares de operación y documentación de las operaciones.

La complejidad de los sistemas y la vulnerabilidad de los programas a cambios, obligan a probar los programas con el propósito de determinar si funcionan de acuerdo a los requerimientos. Por todas estas razones es necesario tener controles de procesamiento fuertes que permitan la detección de errores en la entrada de datos y en el procesamiento.

El procesamiento adecuado requiere de pruebas de validación para detectar errores en los datos, para lo cual se utilizan las siguientes técnicas:

Chequeos de Archivos, a fin de determinar si se esta utilizando el archivo correcto.

- Pruebas de Identificación de registros, para asegurar que el próximo registro a procesar es lógicamente el válido.
- Pruebas de Transacciones, con el propósito de determinar si se están utilizando las rutinas de procesamiento adecuadas.
- Pruebas de Secuencia, a fin de verificar la secuencia de los archivos comparando la clave primaria de cada transacción o registro que es leída con la clave primaria de la transacción o registro anterior.

Al completar el procesamiento es necesario balancear los totales de control con el propósito de detectar transacciones equivocadas, incompletas o duplicadas. Estos totales de control incluyen

- Totales entre subsistemas, es decir los totales de control de un subsistema es comparado con los totales de control de otro subsistema.
- Totales de Corrida a Corrida, son totales de control que requieren de los totales de control previos para terminar el procesamiento.

La corrección de errores durante el procesamiento requiere de procedimientos de corrección y reprocesamiento, un adecuado rastro de auditoria para cada aplicación y de puntos de chequeo. Adicionalmente en casos de desastres es necesario contar con un Plan de Recuperación a fin de regenerar todas las transacciones y los archivos maestros, y restaurar el procesamiento sin errores o pérdida de data.

Los procedimientos de corrección y reprocesamiento son de dos tipos: cuando un error es detectado por las pruebas de validación de procesamiento y cuando el error es detectado posteriormente al procesamiento debido a una revisión manual del procesamiento o por conciliación de los totales de control

El Auditor de Sistemas utiliza las pistas de auditorías del procesamiento, el cual es un cuadro de los eventos que ocurre durante el procesamiento. Solamente en los sistemas simples estos eventos están completamente documentados. En la mayoría de sistemas es necesario revisar el log del proceso y data, así como la lógica que usa el programa.

Los puntos de chequeos son utilizados por el Auditor de Sistemas como puntos intermedios en el procesamiento que van a permitir identificar en que parte del procesamiento ha ocurrido un error, facilitando la corrección del error y su reprocesamiento a partir de dicho punto, evitando de esta manera un reproceso completo.

2.6.3 PROCESO DE CONTROL DE LA SALIDA

Estos controles están relacionados con impresión de reportes, así como la presentación visual de la información. Acceder a reportes no autorizados crea un riesgo de pérdida de activos o de información vital, los mismos que pueden ser controlados mediante procedimientos de manejo de reportes y control de los terminales.

Los procedimientos de distribución de reportes deben estar especificados en la documentación de operaciones de cada aplicación así como la lista de usuarios a quienes se les va a distribuir los reportes. Estos procedimientos deben incluir:

Lista de distribución

Frecuencia de distribución

Log de distribución

La restricción a los terminales de usuarios no autorizados están incluidas en la restricciones fisicas de acceso a los terminales, restricción en el acceso a los departamentos y un control de los passwords.

2.7 AUDITORIA DEL CENTRO DE PROCESAMIENTO DE INFORMACIÓN

El Centro de Procesamiento de la Información es el encargado de controlar el normal funcionamiento de los sistemas y de los equipos (software y hardware). Los ambientes de procesamiento de información varían en las distintas organizaciones según el tamaño del computador y de la carga de trabajo.

En esta etapa el Auditor de Sistemas tiene que evaluar el grado de cumplimiento de los procedimientos para

Administrar y Ejecutar Programas de Producción

Administrar Problemas

Monitorear el Uso Eficaz y Eficiente de los Recursos

Controlar la Entrada/Salida de Datos

2.7.1 CONTROL DE LOS PROCEDIMIENTOS PARA ADMINISTRAR Y EJECUTAR PROGRAMAS ES PRODUCCIÓN

El Auditor de Sistemas debe revisar la documentación de las operaciones, las cuales deben incluir la información necesaria para que el personal de operaciones opere, mantenga y resuelva problemas. Esta documentación debe incluir los procedimientos de asignación de trabajo, con el propósito de garantizar una utilización óptima de los requerimientos de procesamiento.

En esta etapa el Auditor de Sistemas debe evaluar el cumplimiento de los procedimientos formales de Pase a Producción de Programas, mediante un control de cambios a los programas, el cual debe comprender:

- Una documentación completa y actualizada, verificando si cumplen las normas establecidas de Sistemas, Operaciones y Programas.
- Revisión de los resultados de las pruebas, con el propósito de verificar que éstos hayan sido probados y aprobados por los usuarios y por el Jefe de Proyecto.
- Evaluar el proceso de conversión de los datos, a fin de la misma se haya realizado de manera exacta y completa.

Los controles sobre los recursos de la biblioteca off-line es importante para garantizar la continuidad de las operaciones en caso de desastres. El acceso no autorizado a dicha información puede originar pérdida de datos, cambios no autorizados y puede tener un impacto sobre la capacidad de operación del centro de procesamiento. Los controles de biblioteca off-line incluyen:

- Controlar el acceso físico a la biblioteca sólo a personal autorizado.
- Verificar que el ambiente es resistente al fuego/calor excesivo (por lo menos 2 horas).
- Verificar que la biblioteca se encuentre separada del Centro de Procesamiento.
- Asegurar que exista un inventario permanente de todas las cintas y archivos almacenados en la biblioteca, verificando que se lleva un registro permanente del contenido de las mismas.

2.7.2 CONTROL DE LOS PROCEDIMIENTOS DE ADMINISTRACIÓN DE PROBLEMAS

La naturaleza extremadamente compleja de Software, Hardware y sus interelaciones, obligan al uso de un registro de control de las actividades de procesamiento (log), con el propósito de detectar y documentar cualquier situación anormal.

El Auditor de Sistemas debe verificar que existan procedimientos para la administración de problemas, con el propósito de garantizar que no existan problemas sin solución, debido a que éstos problemas pueden ser la causante de pérdida de la continuidad funcional del negocio. Asimismo, es necesario verificar que los problemas deben ser comunicados al personal correspondiente a fin de dar solución al mismo en el menor tiempo posible.

2.7.3 CONTROL DE LOS PROCEDIMIENTOS PARA MONITOREAR EL USO EFICAZ Y EFICIENTE DE LOS RECURSOS

El control eficaz de los recursos del computador es importante debido a dependencia del procesamiento informático para la administración del negocio. Los recursos del computador incluyen hardware, software, telecomunicaciones y datos.

Los procedimientos para monitoreo de hardware incluyen :

- Informes de disponibilidad del computador , a fin de determinar la inactividad del centro de procesamiento. También se denomina "down time"
- Informes de utilización de CPU: procesadores, canales, medios de almacenamiento secundario. La utilización de recursos debe rondar entre el 85% al 95%.
- Verificar la existencia de un programa de mantenimiento hardware, con el propósito de asegurar su correcto funcionamiento. Se debe verificar los costos de mantenimiento excesivos o que superan el presupuesto.
- Verificar que exista una adecuada planificación de la capacidad del computador, a fin de anticipar futuras necesidades de hardware a partir de las necesidades proyectadas. La planificación de la capacidad debe incluir:

  Utilización de CPU

  Utilización de almacenamiento del computador

Utilización de Terminales

Número de Usuarios

Nuevas Tecnologías

Nuevas Aplicaciones

Acuerdos de Niveles de Servicio

Revisión de los informes de error del hardware para poder asegurar el correcto funcionamiento de los equipos.

Como consecuencia de que las casas de desarrollo de software constantemente mejoran y amplían su producto, es importante que el Auditor de Sistemas verifique que se esta utilizando una versión actualizada del Software, con el propósito de evitar de que el software se convierta en obsoleto y sea incompatible con los requerimientos de las innovaciones tecnológicas que suelen acompañar la incorporación de nuevas aplicaciones.

Las telecomunicaciones brindan a los usuarios la posibilidad de tener un acceso a información almacenada en computadores remoto, sin embargo la implantación de esta tecnología es muy costosa por el hardware y software que requiere. Es por esta razón que el Auditor de Sistemas debe evaluar el uso eficiente y eficaz de las funciones de las telecomunicaciones controlando lo siguiente:

El tiempo de respuesta del computador, con el propósito de determinar si éstos se encuentran dentro de los rangos aceptables.

El tipo de transmisiones de telecomunicaciones y verificar si éstas terminan correctamente.

El éxito del centro de procesamiento depende de satisfacer los requerimientos de procesamiento y de los servicios a los usuarios finales, los cuales incluyen que la salida relacionadas con las aplicaciones procesadas sean exacto, completo,

oportuno y distribuido correctamente, para ello el Auditor de Sistemas debe revisar:

Informes de terminación anormal de los trabajos, los cuales se pueden deber al pobre diseño, codificación y pruebas de las aplicaciones, instrucciones de operación inadecuadas, etc. Es necesario tener en cuenta el informe de ejecución de procesos, para identificar la repeticiones o reinicio de procesos.

Problemas de operaciones del computador y sus soluciones, para determinar si las acciones del operador fueron adecuadas o si se debe dar entrenamiento adicional a los operadores.

Planillas de trabajo del operador , como ayuda para la planificación de los recursos humanos y de esta manera asegurar de que se satisfacen los requerimientos de los usuarios finales.

Planillas de trabajo, a fin de permitir una utilización eficiente de los recursos del computador y mantener las demandas de los usuarios en un nivel manejable y a la vez permitir que se procesen trabajos no programados o a pedido sin demora innecesaria.

2.8 AUDITORIA DE LA SEGURIDAD DE LA INFORMACIÓN

La Seguridad de la Información son controles generales implantados con el propósito de prevenir o detectar fallas en el sistema de seguridad, considerando un plan de recuperación en caso de que ocurran estas fallas. Un buen sistema de seguridad debe contemplar procedimientos para minimizar el impacto de las fallas.

Es imposible salvaguardar un computador con simples restricciones fisicas de acceso a programas, data y equipos. El uso de terminales on-line y del proceso de comunicación de datos permite el acceso no autorizado al computador por personas que nunca han pisado el centro de cómputo.

El objetivo es analizar los controles establecidos con el fin de proteger el centro de cómputo frente amenazas accidentales, intencionales y naturales, así como el uso indebido o destrucción.

2.8.1 CONTROLES QUE PROPORCIONAN UN SISTEMA DE SEGURIDAD

El principal objetivo de un sistema de seguridad es reducir la probabilidad de que el sistema falle. Los controles que ayudan a cumplir este objetivo son: Administración de la Seguridad, Facilidades de Control , Control de Librerías y Control de Acceso On-line.

2.8.1.1 ADMINISTRACIÓN DE LA SEGURIDAD

La planificación de un Sistema de Seguridad permiten establecer el máximo beneficio a los controles, incrementando la probabilidad de que éstos funcionen en casos de fallas del sistema. El primer paso es establecer los objetivos de seguridad, con el fin de proporcionar estándares que nos permitan evaluar la probabilidad de ocurrencia de un riesgo, así como el costo a incurrir en caso de que éste ocurriese.

Aquí es donde se desarrolla un plan que permita un nivel de seguridad a un costo razonable. El plan describe todos los controles y los propósitos de su inclusión en el mismo, siendo necesario ser revisado y aprobado antes de su implantación. Los resultados de estas pruebas permiten evaluar la efectividad de los controles.

2.8.1.2 FACILIDADES DE CONTROL

Las facilidades de control están diseñadas para proteger el centro de cómputo y los equipos de daños fisicos, los cuales a su vez pueden causar la

pérdida de la capacidad de procesamiento y causar daño o pérdida de data vital, programas y documentación.

Los controles de ubicación y de construcción, son factores que permiten reducir el riesgo. El centro de cómputo puede estar ubicado en un edificio separado o en un ambiente seguro dentro de la institución, contribuyendo también los estándares de construcción a reducir el riesgo: las puertas deberían ser fuertes y los vidrios deben evitarse en lo posible o en su defecto deben estar protegidos con una película antiimpacto.

Los controles de acceso son necesarios para prevenir el acceso no autorizado. Un cerco perimetral constituye una primera línea de defensa, pero al mismo tiempo es necesario contar con varios procedimientos de seguridad y dispositivos que limiten al personal el acceso al centro de cómputo.

2.8.1.3 CONTROL DE LIBRERÍAS

Los controles de librerías restringen el acceso a data, programas y documentación. Los controles físicos sobre los archivos usados permiten protegerlos de daño durante su manipulación. Estos controles son:

- Cabecera Interna y Etiquetas de Control que pueden ser leídas por el sistema para asegurar que se esta procesando el archivo correcto. También permite determinar que archivo se ha leído completamente y que registro ha sido perdido o adicionado.
- Etiquetas Externas, las cuales proporcionan una confirmación visible al operador de que se esta utilizando el archivo correcto.
- Switch de Solo Lectura.

2.8.1.4 CONTROL DE ACCESO ON-LINE

Los controles físicos de acceso al computador proveen un nivel de seguridad a los sistemas en batch, pero sin embargo es insuficiente para un sistema en línea donde los terminales se encuentran distribuidos a través de toda la empresa.

El acceso físico a los terminales debería restringuirse en lo posible, mediante el bloqueo de terminales. Los programas y data deberían estar controlados por esquemas de autorización, que permitan sólo el acceso a usuarios autorizados. El propósito del esquema de autorización es restringir el acceso al sistema sólo a terminales autorizados y a usuarios autorizados.

El esquema de autorización debería prevenir el acceso de terminales ilícitos, mediante una lista de todos los terminales autorizados a usar el sistema. El acceso de un terminal que no aparece en esta lista debe negársele el acceso.

El esquema de autorización debería identificar los programas y archívos de datos que cada usuario esta permitido accesar. Este acceso esta basado en la responsabilidad funcional y en la autorización para leer data confindencial.

Para que el esquema de autorización sea efectivo, es necesario complementarlo con un método de identificación del terminal y del usuario, el cual va acompañado de un password. La identificación del terminal asegura que el terminal usado esta autorizado.

El control de acceso a los terminales no es efectivo en un sistema on-line a menos que la comunicación de data este también restringida. Los controles para reducir el daño sistema de comunicación de datos incluye:

- Fragmentación, el envío de información en fragmentos.
- Intermixing, el envío de diferentes paquetes de información a la vez.
- Encriptación, el cual es la codificación de la data para encubrir su significado.

2.8.2 CONTROLES PARA DETECTAR FALLAS EN EL SISTEMA DE SEGURIDAD

Los controles que proveen de una seguridad al sistema no proporcionan una seguridad absoluta, pero si pueden reducir la probabilidad de ocurrencia de fallas. Los controles de detección proporciona la oportunidad de reducir daños o pérdida en caso de que la seguridad falle, utilizando dispositivos de detección, autenticación y monitoreo del sistema.

Los dispositivos de detección son dispositivos electrónicos o mecánicos que permiten detectar fuego o acceso no autorizado. El propósito es proporcionar una oportunidad para minimizar el daño o pérdida.

La autenticación permite la identificación correcta del usuario que accesa a un sistema con propósitos autorizados, sin embargo, esto no asegura el uso del sistema por dicha persona, obligando al uso de controles de autenticación posteriores a la identificación inicial.

El monitoreo del sistema permite detectar la ruptura de la seguridad, mediante una revisión del log del sistema de todas las fallas y otras violaciones de los procedimientos de seguridad, accesos insatisfactorios al sistema y cámaras que permitan monitorear la actividad del ambiente del centro de cómputo.

2.8.3 CONTROLES DE RECUPERACION

Un sistema de procesamiento de datos debe tener controles que aseguren una efectiva recuperación en caso de que el sistema falle.

El daño por fuego puede ser minimizado mediante una cuidadosa selección y diseño de sistemas contra incendios. El ambiente de procesamiento de datos debe estar seguro mediante la ubicación estratégica de extintores de operación manual o automático.

Es necesario tomar seguros adecuados que cubran la información y los equipos, para reducir la probabilidad de interrupción del negocio.

Un Plan de Recuperación formal representa un elemento esencial para la recuperación, asegurando que se han evaluado las posibilidades de que un sistema falle y se han diseñado estos procedimientos con el propósito de minimizar la pérdida de datos y activos. Los procedimientos de recuperación debe incluir:

- Facilidades del computador y Equipos, es necesario contar con backups de los facilidades del computador y de los equipos, con el fin de proporcionar el servicio durante el tiempo que demore la contingencia.
- Software, el plan de recuperación debe asegurar que se cuenta disponible una copia de seguridad del software y de los manuales del mismo.
- Data, el plan de recuperación debe permitir la reconstrucción de archivos maestros, archivos de transacciones, y documentos fuentes.
- Personal, el plan de recuperación debe identificar al personal responsable de cada tarea.
- Abastecimientos, el plan de recuperación debe incluir un inventario de las material de procesamiento de datos requeridos en situaciones de emergencia.

CAPITULO III : APLICACIÓN PRACTICA

3.1 SISTEMA DE PROCESAMIENTO

Para la SUNAT el tiempo de respuesta de los procesos es el aspecto más crítico en el procesamiento de datos, el cual se vuelve más crítico aún a medida que el volumen de información se vaya incrementando. Con el propósito de disminuir el tiempo de respuesta, la Intendencia Nacional de Informática ha optada por la utilización del concepto de Procesamiento Distribuido, con la finalidad de distribuir el procesamiento en las Dependencias del interior del país, debido a que es aquí donde se generan las transacciones.

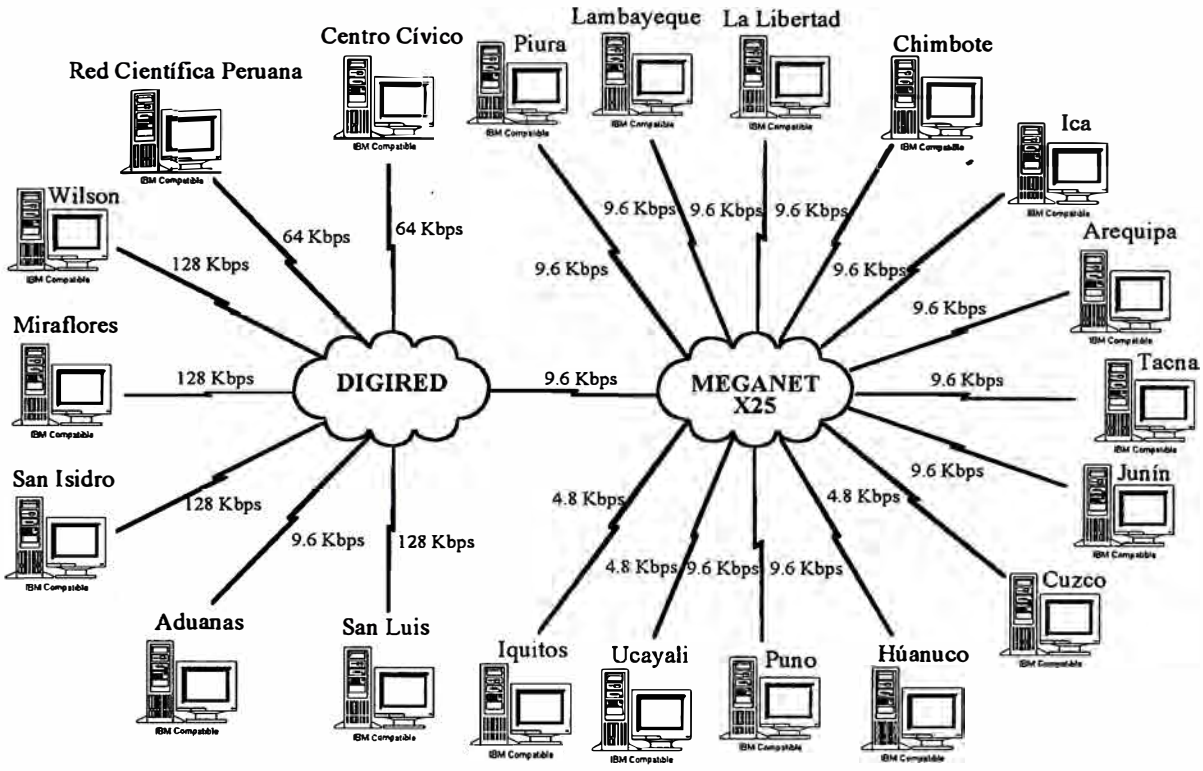
El Departamento de Soporte Técnico ha diseñado y administra actualmente los servicios de transmisión de información (Data) entre la Regionales y Zonales a través de la **Red de Datos SUNAT.** Para ello utiliza los siguientes servicios que brinda Telefónica del Perú:

1. DIGIRED, el cual permite enlazar los locales de Wilson - San Isidro - Miraflores , formando una configuración delta. Así mismo se encuentran interconectados los locales de Centro Cívico, San Luis, Aduanas y la Red Científica Peruana. Es una red de reciente tecnología, el cual permite una comunicación fluida (velocidades de transmisión **hasta 2048 Kbps**) que se basa en la comunicación puntual.
2. MEGANET, para la interconexión de la Regionales y Zonales. Es una red antigua y lenta (hasta 9.6 Kpbs), cuya arquitectura se basa en la conmutación de paquetes.

Así mismo, a través de la **Red de Datos SUNAT**, se transmite información cuyo volumen esta en constante crecimiento: envío de programas, Novedades Prico,

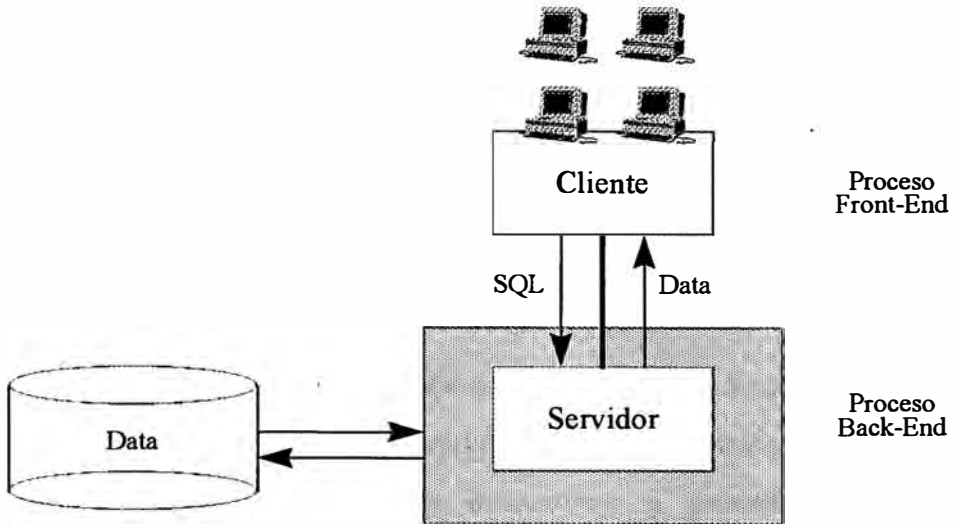
Novedades Mepeco, Novedades RUC, Consulta a red bancaria, etc., por lo tanto se necesita no sólo una red veloz sino equipamiento necesario para soportar el crecimiento del flujo de información.

Figura 3.1 : Red de Datos SUNAT



Debido a que los requerimientos de procesamiento de la información es en línea para el Sistema de Principales Contribuyentes, el Sistema de RUC y el Sistema de Comprobantes de Pago, se esta utilizando la arquitectura Cliente/Servidor, debido a que permite obtener un menor tiempo de respuesta. Este tipo de arquitectura usa dos procesos separados : el front-end el cual provee de una interface para los usuarios y el back-end administra el manejo de toda la data.

Figura 3.2 : Arquitectura Cliente/Servidor



La arquitectura cliente servidor permite ofrecer varias ventajas:

- Incremento de la performance, debido a la separación de los procesos de front-end y back-end, lo cual permite que hardware y software sean utilizados para tareas específicas.
- Mayor flexibilidad, debido a que se pueden utilizar diferentes servidores de data, permitiendo utilizar una arquitectura abierta.
- Reducción de Costos, debido a que el hardware puede ser seleccionado para encajar de acuerdo al tamaño de la aplicación.
- Portabilidad, las aplicaciones pueden ser a diferentes máquinas fácilmente.

3.2 CENTRO DE PROCESAMIENTO DE LA INFORMACIÓN

Los Centros de Procesamiento de la Información de las dependencias del interior del país esta a cargo de dos personas: El Supervisor del Centro de Cómputo y del Analista de Operaciones.

Las funciones del Supervisor del Centro Cómputo son las siguientes:

1. Ejecución de procesos a solicitud del Dpto. de Soporte Técnico o del Departamento. de Operaciones.
2. Absolución de los problemas presentados con las Aplicaciones, con el Sistema Operativo, Software de Aplicación para PCs, configuración de impresoras y de teclados, y coordinación con Lima para aquellos problemas que no pueden ser resueltos hasta su adecuada solución.
3. Brindar la información requerida por los usuarios de la Intendencia Regional u Oficinas Zonales en reportes o DBFs.
4. Verificación permanente del espacio en disco y file systems, funcionamiento de los puertos, funcionamiento del equipo de cómputo, comunicación via x25.
5. Mantenimiento actualizado de instructivos y procedimientos de los procesos obligatorios diarios, semanales o mensuales, así como su adecuación para hacer su ejecución rápido.
6. Otorgar accesos a la Base de Datos.

Las funciones del Analista de Operaciones son

1. Administración de la Cintoteca.
2. Ejecución de los procesos obligatorios diarios, semanales y/o mensuales.
3. Actualización de las Bases de Datos con datos de la Red Bancaria para la Intendencia Regional y Oficinas Zonales de su jurisdicción.
4. Realización de los niveles de BackUps de las Bases de Datos y File Systems, etc. llevando un adecuado control de los mismos.
5. Ejecutar pedidos de impresión de los usuarios.
6. Corrección de la información de la Base de Datos debidamente autorizadas.
7. Control y archivo documentario.

Los requerimientos de hardware requeridos por una dependencia del interior del país es de un Host principal donde se encuentran las principales bases de datos y un servidor adicional donde se almacena una copia de las bases de datos más importantes. Adicionalmente, se utiliza un servidor por cada Oficina Zonal que corresponda a la jurisdicción de la Intendencia Regional.

Cuadro 3.1 : Configuración del Hardware

	Host	***Servidor***	***Servidor Zonal***
Modelo	NCR 3420	NCR 3410	AST Premia SE P/60
Procesador	Pentium 60 Mhz	486/66 Mhz	Pentium 60 Mhz
Nro. de CPU	1	1	1
Memoria	32 Mb.	32 Mb.	32 Mb.
Discos	2 discos de 2 Gb. 1 Disco de 1 Gb.	2 discos de 1 Gb. 1 Disco de 200 Mb.	1 discos de 1 Gb. 1 Disco de 500 Mb.

La SUNAT utiliza como Sistema Operativo Base el UNIX, utilizándose el System V para los computadores de una Intendencia Regional y el SCO para los computadores utilizados por una Oficina Zonal. El Administrador de Base de Datos es el Informix, debido a que se adapta a los requerimientos de procesamiento de información requeridos por la institución.

Cuadro 3.2 : Configuración del Software Base

	Host	***Servidor***	***Servidor Zonal***
Sistema Operativo	UNIX System V Release 2.02	UNIX System V Release 2.02	UNIX SCO
Base de Datos	Informix On-Line Informix 4gl Informix SQL	Informix On-Line Informix 4gl Informix SQL	Informix On-Line Informix 4gl Informix SQL

El cuadro que se muestra a continuación permite observar como están organizadas las Bases de Datos utilizadas por la institución. Una característica básica es que los datos pueden ser compartidos por todos los usuarios, siendo necesario un Administrador de la Base de Datos a fin de evitar conflictos a nivel de recursos e información.

Cuadro 3.3 : Configuración las Base de Datos

On-Line	*Host*	*Servidor*	*Servidor Zonal*
tbconfig.prico	SIRAT (PRICOS)	SIRAT (PRICOS)	
tbconfig.bancos	Recauda (MEPECOS) SIRAT (DV)		Recauda (MEPECOS)
tbconfig.cp	recauda (RUC y CP PRICOS)	recauda (RUC y CP PRICOS)	

3.3 SISTEMAS DE RECAUDACION

Hasta Agosto de 1992, la Recaudación se manejaba con el Sistema de la Oficina de Informática y Estadística del Ministerio de Economía y Finanzas, el cual presentaba las siguientes características:

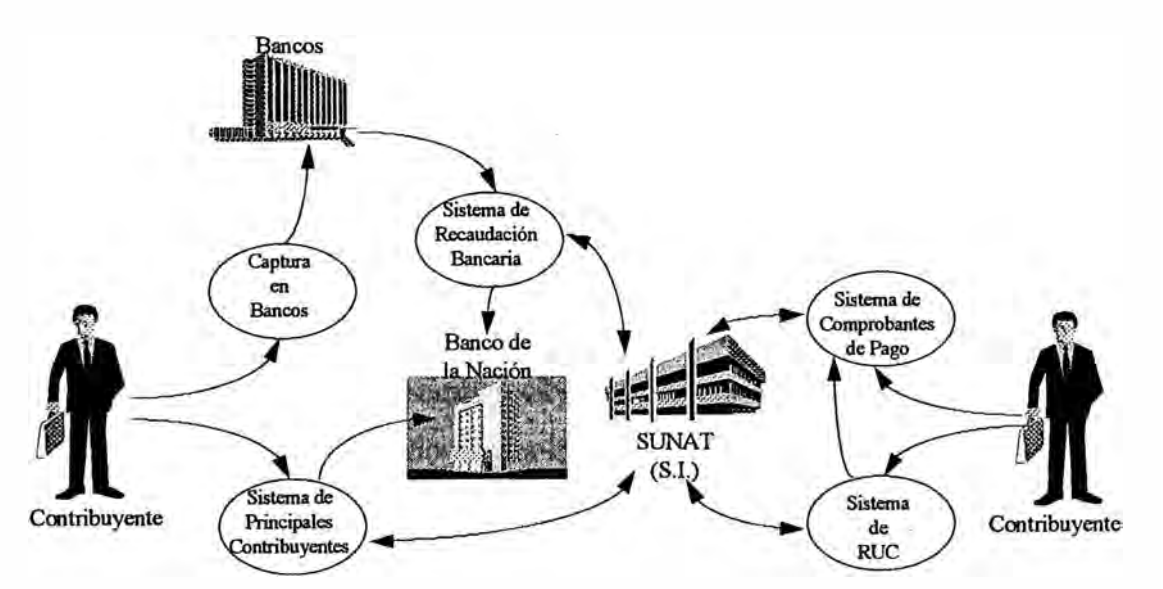
1. Emisión de Libretas Tributarias sin restricciones se efectuaba en tres dependencias: Lima, Arequipa y Trujillo.
2. Padrón de Contribuyentes dividido e 2: Padrón Antiguo (entre 1965 y 1985) con vacíos e inconsistencias y Padrón Nuevo (entre 1986 y mediados de 1992), el cual limitaba la emisión.
3. El Banco de la Nación era la única entidad bancaria que podía recaudar.
4. Toda la información era remitida a Lima para su ingreso y procesamiento.
5. El arqueo del Banco de la Nación era manual y la información inconsistente y desactualizada.
6. Emisión de valores selectiva, según la importancia de los contribuyentes.
7. No había la certeza de los pagos efectuados por los contribuyentes.

Todos estos factores contribuyeron a una pobre recaudación y a la baja percepción de riesgo en la labor de SUNAT.

A partir de Agosto de 1992 se inicia un nuevo control de los Sistemas de Recaudación por parte de SUNAT con los siguientes objetivos:

1. Identificar a los contribuyentes y categorizarlos (Sistema RUC)
2. Determinar los mecanismos de control y seguimiento de la deuda de los contribuyentes (Sistema de Recaudación de Principales Contribuyentes y Sistemas de Recaudación Bancaria).
3. Controlar el cumplimiento de las obligaciones formales de los contribuyentes.

Figura 3.3 : Sistema Integrado de Procesamiento de la Información



3.3.1 SISTEMAS DE RECAUDACION DE PRINCIPALES CONTRIBUYENTES

En Agosto de 1992 se crea el Sistema de PRICOS en la Intendencia de Principales Contribuyentes Nacionales, controlándose a 1692 contribuyentes que representan un importante porcentaje de la recaudación nacional. Posteriormente se ha implantado un sistema de Réplicas de la Estructura de PRICOS en las dependencias del interior del país.

El Sistema de Principales Contribuyentes tiene los siguientes propósitos:

1. Control más eficiente del cumplimiento de las obligaciones tributarias de los PRICOS, facilitando las labores de recaudación y fiscalización.
2. Mejor servicio al contribuyente.

El Sistema de Principales Contribuyentes permite ingresar en línea la información de las declaraciones presentadas por los contribuyentes, procesar dicha información (reliquidar), controlar los aspectos de cumplimiento y finalmente dar seguimiento a las obligaciones de los contribuyentes.

El proceso de la información se inicia con la identificación y la naturaleza tributaria del contribuyente. El sistema recibe las declaraciones, las reliquida e informa de las diferencias. Luego de ello asigna lo ingresado por contribuyente, tributo, período y documento.

La siguiente etapa de este proceso es determinar los Omisos a la Presentación, según su vector fiscal particular , con el propósito de emitirles Esquelas de Notificación y las Resoluciones de Multas. A los Omisos al Pago total o parcial, el sistema les emite Ordenes de Pago.

Luego de cumplirse el plazo de ley, el sistema traslada los valores no pagados a los procedimientos de cobranza coactiva, con el propósito de recuperar las deudas morosas de los contribuyentes.

En la última etapa, se procesa la información relacionada con las solicitudes de fraccionamiento que realizan los contribuyentes con el fin de cubrir sus deudas pendientes.

Todo esto permite actualizar la Cuenta Tributaria del Contribuyente, el cual consiste en llevar el registro de un conjunto de transacciones con el propósito de determinar el saldo del contribuyente en base a los débitos y créditos generados por dichas transacciones.

3.3.1.1 DESCRIPCION DEL SISTEMA

El sistema ha sido desarrollado en forma modular, pero conservando la relación e integración entre sus módulos, permitiendo de esta manera completar el ciclo de procesamiento de la información. El Sistema cuenta con los siguientes módulos:

1. Directorio de Contribuyentes: Permite administrar y controlar la información básica del contribuyente:

   Identificación del Contribuyente: Nombre o Razón Social.

   Establecimientos Anexos y Representantes Legales.

   Tributos a los que se encuentra afecto.

   Adicionalmente, en este módulo se almacena información histórica del Vector Fiscal del Contribuyente como son los tributos a los cuales se encuentran afectos, los períodos de exoneración y sistemas de pago.

2. Captura de Documentos: Este módulo esta parametrizado y flexible como respuesta a los constantes cambios debido a los ajustes

originados por las Normas Legales y por los nuevos formularios. Permite capturar la información de los formularios en forma rápida y sencilla. El sistema cuenta con opciones de :

- Captura de Datos.
- Validación en línea.
- Reliquidación de la declaraciones juradas, controlando la correcta utilización de los saldos a favor, así como los pagos anticipados realizados por el contribuyente.
- Actualización de la deuda del contribuyente, calculando los intereses moratorios.
- Control de las Declaraciones Juradas Rectificatorias, tomando el pago de la Declaración Jurada Original como un pago a cuenta.

3. Caja: Permite recibir los pagos de las Declaración Jurada y Boletas de Pago, cuya información ha sido introducida por el receptor en el módulo de Captura de Documentos. Adicionalmente refrenda los documentos y emite los comprobantes de pago correspondientes. Este módulo permite:

- Cumplir con los requerimientos de una caja bancaria: apertura y cierre.
- Refrendo de comprobantes y arqueo de cajas en las diferentes formas de pago (efectivo, cheques, documentos valorados y notas de crédito).
- Genera Notas de Débito por la comisión que le corresponde al Banco por el concepto de recaudación.
- Actualiza la Cuenta Tributaria del Contribuyente.
- Distribuye lo recaudado en el Día por Ente Beneficiario.
- Prepara Novedades de Notas de Abono para el Sistema Central.

4. Documentos Valorados : Permite registrar los documentos valorados utilizados por el contribuyente, como deducción del monto de su deuda determinada en su Declaración Jurada. Este módulo permite distribuir la recaudación en valores a cada uno de los Entes Beneficiarios y también complementar en la cuenta tributaria del contribuyente los pagos realizados con este tipo de documentos.
5. Acreditación a Entes Beneficiarios : Permite realizar la distribución de la recaudación del día a los diferentes entes beneficiarios, por medio de Notas de Abono que respaldan dicha distribución.
6. Omisos a la Presentación : Determina el universo de contribuyentes que han omitido el cumplimiento de sus obligaciones tributarias, tomando como base los tributos a los que se encuentra afectos los contribuyentes y la información presentada en su Declaración Jurada. Este módulo permite:

   Generar las notificaciones (Esquelas).

   Registrar las fechas de Notificación.

   Realizar un seguimiento de las notificaciones.

   Generar las Ordenes de Pago por Presunción[9] en base a los pagos realizados en los últimos 12 meses.

6. Pagos Pendientes : Permite determinar los saldos deudores pendientes de pago, en base a la información proporcionada por el Proceso de Reliquidación. Además este módulo permite:

   Calcular los intereses moratorios de la deuda

   Generar los Ordenes de Pago

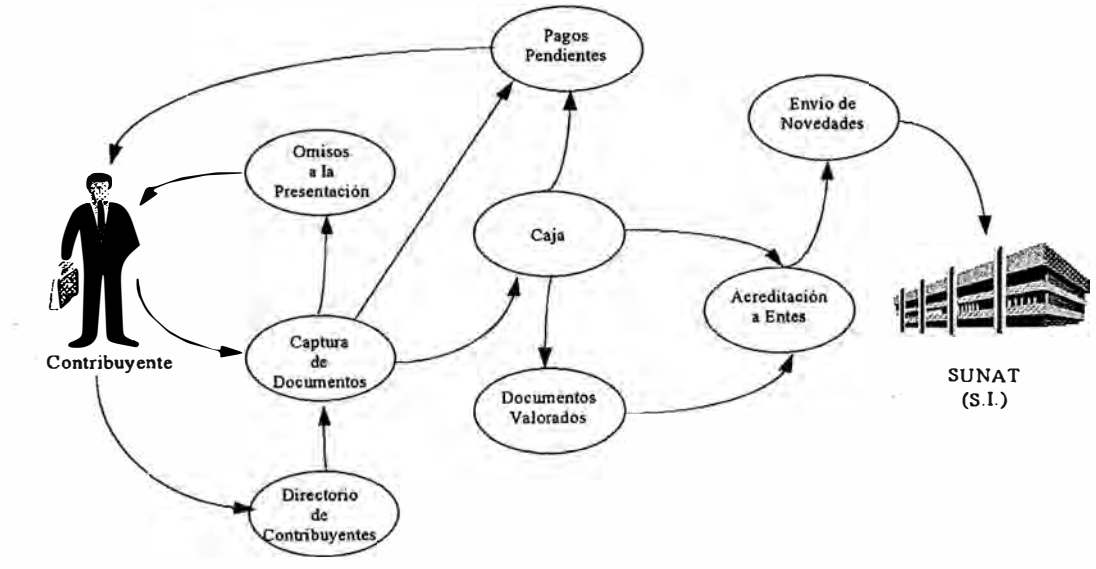
   Registrar las fecha de notificación de las Ordenes de Pago y realizar un seguimiento a las mismas.

---

[9] Una Orden de Pago por Presunción se produce cuando se agotan todas las vías de notificación autorizadas

7. Cobranza Coactiva : Permite controlar y realizar un seguimiento a las Ordenes de Pago y Resolución de Determinación transferidas al Área de Cobranza Coactiva.
8. Fraccionamiento : Este módulo lleva el control de las deudas que han sido fraccionadas en cuotas, previa autorización por parte de la SUNAT.
9. Multas : Permite generar en forma automática las Resoluciones de Multa, por los diferentes motivos: Omisos a la Presentación, Omisos al Pago y por presentar más de una Declaración Jurada Rectificatoria.
10. Novedades desde la Regional : Proporciona Información de las Novedades del Sistema de Principales Contribuyentes, creando archivos planos que son transferidos en forma remota o local al Sistema Central de SUNAT.

Figura 3.4 : Sistema de Principales Contribuyentes



3.3.2 SISTEMA DE RECAUDACION BANCARIA

Hasta el 01 de Julio de 1993, el Sistema de Recaudación carecía de un universo confiable de contribuyentes, existían muchos tributos y la información de sus pagos era inconsistente y el sistema de procesamiento presentaba muchas inconsistencias. Gracias a la facultad que le brinda un dispositivo de Código Tributario, a partir de esa fecha se firman convenios con algunos bancos del país.

Este Sistema esta dirigido a los medianos y pequeños contribuyentes, con la finalidad de facilitarles los pagos. Para ello, la SUNAT firma el Convenio de Recaudación a través de la Red Bancaria, encargando la recepción de Declaración Jurada, Pagos y el Procesamiento de la Información a los bancos.

Los bancos prestan las siguientes labores o servicios:

Reciben los Declaración Jurada de los contribuyentes.

Procesan las Declaración Jurada presentados por los contribuyentes.

Determinan y realizan la transferencia de fondos a las cuentas de los entes beneficiarios.

Entregan los medios magnéticos y los formularios procesados a SUNAT

Por su parte SUNAT abona lo siguiente:

Por el cobro y transferencia de fondos: 1/8 % del total recaudado.

Por la captura y transcripción a medios magnéticos:

2,23 por cada formulario de mas de 30 casillas

1.2 por cada formulario de 30 o menos casillas.

Este sistema se caracteriza por:

Muchos puntos de atención: es decir los Bancos recepciónan los formularios en todas las agencias.

No se controla que la presentación o pago se efectúe dentro del vencimiento establecido.

Cada Ente Beneficiario tiene una subcuenta en el Banco de la Nación, la cual es utilizada únicamente para el abono de la recaudación.

Según el tipo de información contenida en el formulario, estos se clasifican en Formularios con datos primarios, debido a que contienen la información necesaria para conocer la recaudación y el abono correspondiente a cada Ente Beneficiario, y Formularios con Datos Primarios y Secundarios, debido a que tienen la información necesaria para determinar correctamente la deuda tributaria.

Los bancos de la Red Bancaria son los encargados de recepcionar los formularios, agrupándolos al final del día en lotes por código de Resumen de Recaudación, ordenándolos por tipo de pago y por número de formulario. Estos formularios son centralizados en la Oficina Principal del Banco para su digitación. Los Datos Primarios son entregados a la SUNAT el mismo día en que se abona la recaudación, debido a que es necesario generar la Nota de Abono para cada ente beneficiario y proceder al abono respectivo. Los Datos Secundarios son entregados a SUNAT dentro de los 9 días hábiles siguientes a la emisión de la Nota de Abono.

La Nota de Débito por cobro y transferencia de fondos (1/8 %) es emitida en el día en que se genera la Notas de Abono. La Nota de Débito por captura y transcripción es emitida junto con los datos secundarios.

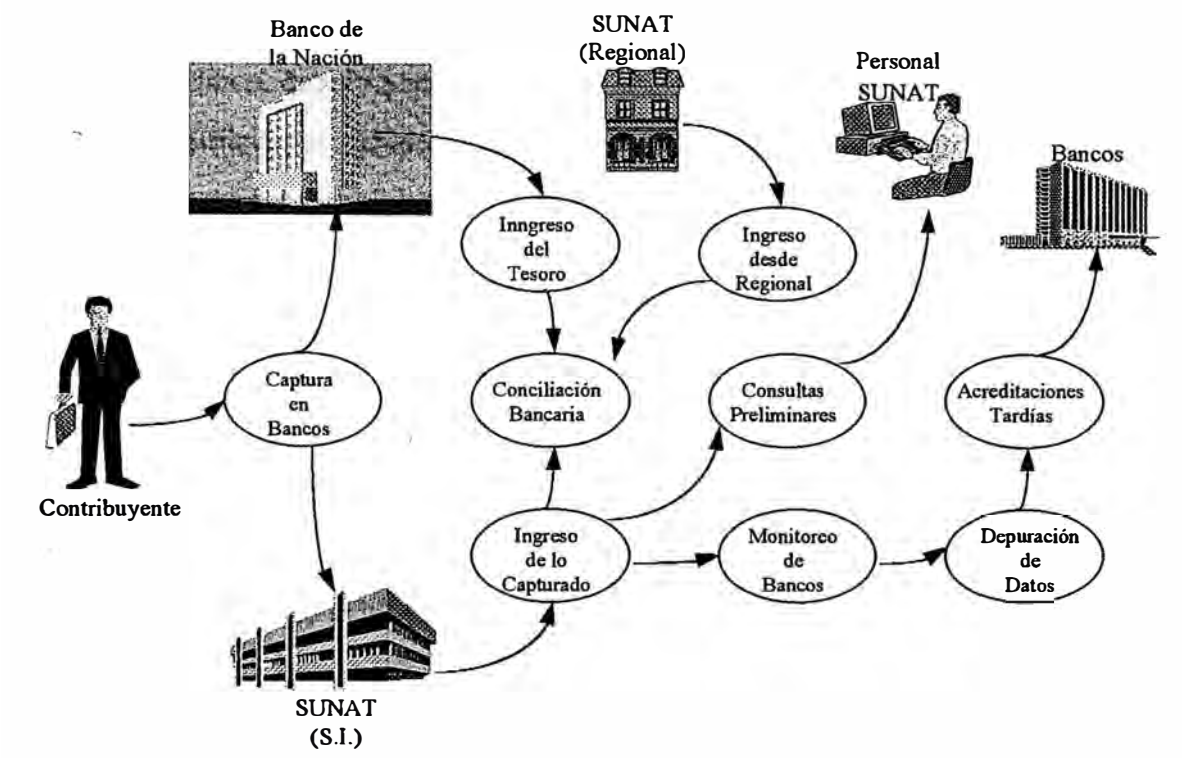
3.3.2.1 DESCRIPCION DEL SISTEMA

Los módulos del Sistema de Red Bancaria son los siguientes:

1. Captura en Bancos : Captura los formularios recepcionados en la Red Bancaria y emite los Resúmenes de Recaudación, Nota de Abono y Nota de Débito. Las funciones son :
   - Captura la información de los formularios presentados por los medianos y pequeños contribuyentes.
   - Emite los Resúmenes de Recaudación por cada lote de documentos Ingresados.
   - Emite las Notas de Abono por cada ente involucrado en la recaudación.
   - Emite las Notas de Débito por cobranza y captura.
2. Ingreso de lo Capturado: Recepciona y valida los medios magnéticos con la información de los Datos Primarios y Datos Secundarios de los formularios provenientes de la Red Bancaria.
3. Ingreso desde el Tesoro : Transfiere al computador central de SUNAT los movimientos imputados a las cuentas fiscales del tesoro. Las funciones que realiza son:
   - Valida y chequea los errores de los datos a transmitir.
   - Carga de los datos a la Base de Datos.
4. Conciliación Bancaria : Concilia los medios magnéticos recepcionados de la Red Bancaria y lo ingresado desde dependencia del interior del país, con los extractos de los entes beneficiarios. Este módulo permite conectarse vía módem con las subcuentas de los Entes beneficiarios abiertas en el Banco de la Nación y cruza dicha información con la remitida por los bancos a SUNAT, conciliando de esta manera la información contenida en los medios magnéticos con lo realmente abonado.

5. Monitoreo de Bancos : Detecta formularios de pagos que no fueron correctamente digitados por los bancos. Comprende los siguientes procesos:
   - Seleccionar los formularios de cada Nota de Abono para que sean digitados en SUNAT.
   - Digitar los formularios seleccionados, reportando las diferencias encontradas.
6. Depuración de Datos : Identifica los datos errados en los formularios y los corrige mediante la depuración del número de RUC y del Período Tributario (solo inversiones de mes y año).
7. Acreditaciones Tardías : Determina la penalidad por el abono extemporáneo de la recaudación y /o entrega tardía de la información (Datos Primarios y Datos Secundarios) a SUNAT. Calcula el monto de la multa y la emisión de la Nota de Abono respectiva.
8. Consultas Preliminares : Permite consultar a través de reportes o pantallas el contenido de las Declaración Jurada o Boletas de Pago presentadas por los contribuyentes de la Red Bancaria o desde las dependencias de PRICOS. Cuenta básicamente con las siguientes características
   - Administrar los formularios que se desean consultar , seleccionando rubros y secciones específicas.
   - Identificar al contribuyente o al formulario a consultar, con criterios de selección para elegir formularios, períodos y orden de la aparición de datos.

Figura 3.4 : Sistema de Recaudación Bancaria



3.3.3 SISTEMA DE REGISTRO UNICO DE CONTRIBUYENTES

La SUNAT antes de implementar este sistema contaba con muchos soportes de información, los cuales se caracterizaban por no contar con un universo actualizado de contribuyentes, la información era poco confiable, existía carencia de información sobre la afectación de tributos y además se utilizan diferentes directorios únicos de contribuyentes. Dada la necesidad de contar con un padrón de contribuyentes controlados por la SUNAT se crea el RUC, cuyo objetivo es mantener un directorio de contribuyentes actualizado.

El Sistema de RUC crea un registro único de contribuyentes , los cuales se encuentran categorizados según su capacidad contributiva e interés fiscal, con el fin

de ejercer eficientemente las labores de recaudación y fiscalización. El RUC se caracteriza por ser:

- Único, debido a que es el único documentos para trámites en la SUNAT.
- Suficiente, debido a que cuenta con toda la información necesaria para conocer la realidad del contribuyente.
- Dinámico, debido a que se actualiza permanentemente.

El Sistema de RUC es un sistema descentralizado en línea, generando una respuesta inmediata a las transacciones de los contribuyentes, mediante el Comprobante de Información Registrada (CIR), el cual a su vez permite realizar otras gestiones como por ejemplo la Autorización de Comprobantes de Pago. Los componentes de la información procesada por este sistema son:

- Datos Principales : Número de RUC, Razón Social, Domicilio Fiscal, CIIU, Fecha de Constitución.
- Datos Secundarios : Teléfonos, Fax, Razón Comercial, Inicio de Actividad.
- Vector Fiscal Particular : Tributos a los que se encuentra afecto o exonerado el contribuyente.
- Representantes Legales Relación de personas que representan a los contribuyentes.
- Establecimientos Anexos: Sedes Productivas, Locales Comerciales, Depósitos.

3.3.4 SISTEMA DE COMPROBANTES DE PAGO

Debido a que las normas relacionadas a la obligación de emitir y entregar comprobantes de pago no cumplían con las necesidades de información requeridas por SUNAT, era imprescindible establecer un sistema integral que permita corregir y brindar un mecanismo acorde con la nueva filosofia de la Administración

Tributaria. Por ello un nuevo sistema computarizado que permitiera conocer el número de comprobantes emitidos y de las obligaciones de su emisión.

El Sistema de Comprobantes de Pago controla el proceso de autorización para la impresión de comprobantes de manera coherente con los tributos a los que se encuentra afecto según el tipo de contribuyente. Asimismo, permite controlar el de impresión realizada por las imprentas autorizadas por SUNAT. Las funciones de este sistema son:

- Captura y validación de la información contenida en los formularios de solicitud de autorización.
- Autorización en Línea, previa validación con el Sistema de RUC.
- Captura de la información proporcionada por las imprentas de los trabajos realizados y confrontación con las autorizaciones otorgadas por los contribuyentes.

Adicionalmente se cuenta con un sistema provisional en PC, para aquellas dependencias que no cuenten con un Sistema en Línea. Este sistema permite capturar y consultar la última autorización de habilitación de comprobantes.

PROCESO DE AUDITORIA DE SISTEMAS

El presente trabajo ayudará a identificar los aspectos que se deben considerar al realizar un Proceso de Auditoría de Sistemas a las dependencias de SUNAT del interior del país. Lo que se describirá a continuación es una guía para su uso en todas las actividades del Centro de Procesamiento de Información, con el propósito de garantizar el funcionamiento adecuado y seguro de los sistemas en producción.

3.4.1 AUDITORIA DE LOS CONTROLES DE ORGANIZACIÓN Y ADMINISTRACIÓN

La efectividad de los procedimientos de control depende las actividades ejecutadas por el personal responsable de ellas, verificándose la aplicación de las normas y procedimientos con el propósito de minimizar los riesgos en las instalaciones, equipos, programas y datos. La labor que debe realizar el Auditor de Sistemas es la siguiente:

1. Verificar que las circulares sobre el Procedimiento de Uso de Formatos de los Procesos Informáticos y Procedimiento de Uso Adecuado de las Computadores Personales y Prevención, Detección y Eliminación de Virus Informáticos hayan sido distribuidos entre todo el personal de la Intendencia Regional u Oficina Zonal.
2. Verificar que los Procedimientos de Manipulación y Cuidados de Data Cartridge y los Procedimientos de BackUp de la Información haya sido distribuido entre el personal de Centro de Cómputo.
3. Evaluar el cumplimiento del Esquema de la Administración de los Sistemas en Producción, el cual brinda el marco de estandarización para:
   - Administración de Cuentas
   - Administración de Directorios
   - Administración de Procesos en Producción
   - Administración de la Transferencia de la Información

4. Verificar la utilización de software original de parte del personal de la Intendencia Regional u Oficina Zonal, con el propósito de evitar el uso de copias no autorizadas[10] y la piratería de software[11] , evitando al mismo tiempo el uso de copias que no ofrecen la calidad y seguridad.
5. Revisar la utilización y archivo de los formatos de Procesos Informáticos, con el propósito de controlar la secuencia de uso y evitar la pérdida de los mismos.
6. Realizar una observación por las áreas que utilizan los servicios del Centro de Procesamiento de Información, con el fin de comprobar la política de escritorio limpio y la política de destrucción de reportes que contienen información.
7. Evaluar el desempeño del personal del Centro de Procesamiento de la Información en los siguientes aspectos:

   Administración del Centro de Procesamiento

   Solución de los problemas de hardware y software

   Atención a los requerimientos de los usuarios : Requerimientos de Información y Requerimientos de Microinformática.
8. Comprobar el servicio brindado por el Centro de Procesamiento de Información y analizar con los usuarios las fortalezas y debilidades de los sistemas.
9. Verificar que la limpieza del Centro de Procesamiento se efectúe bajo la supervisión del personal del mismo.

---

10 Copia no Autorizada, es cualquier copia del software original que no haya sido autorizada por casa de software que lo desarrolló.

11 Piratería de Software, significa el uso de un software distinta a la permitida por la legislación de los derechos de autor o a la licencia de software.

10. Evaluar el área asignada para el Centro de Procesamiento de Información y la distribución de la Red de Datos con la finalidad de que esta se extienda a través de todas las áreas usuarias, o en caso contrario recomendar una ampliación de los mismos..
11. Evaluar los requerimientos de hardware de la Intendencia Regional u Oficina Zonal, con el propósito de elevarlos al Departamento de Soporte Técnico a fin de considerarlos en el Plan Anual de Adquisición de Equipos.
12. Evaluar el cumplimiento del cronograma y servicio de Mantenimiento Preventivo de Equipos realizados por los proveedores de SUNAT.

3.4.2 AUDITORIA DEL PROCESO DE CAMBIOS A LOS PROGRAMAS

El personal de Centro de Procesamiento de la Información, realiza una labor básicamente operativa, dejando las labores de desarrollo y mantenimiento de los sistemas para el personal de informática en Lima, motivo por el cual no se ha considerado la totalidad del Proceso de Auditoría para el Ciclo de Desarrollo de Sistemas. El personal de estas dependencias generalmente realiza la Instalación de los Nuevos Sistemas y en un mayor número la Ejecución de Procesos Batch Extraordinarios y de Queries que actualizan las bases de datos.

Después de que un sistema nuevo ha sido puesto en producción, el Auditor de Sistemas debe realizar un control de los mismos, el cual incluya:

1. Verificar que los Pases a Producción, Ejecución de Procesos Batch Extraordinarios y Ejecución de Queries, se encuentren debidamente sustentados en los formatos correspondientes, llevándose un registro cronológico de todos los cambios efectuados.

2. Asegurar que el personal del Centro de Procesamiento de la Información realiza sólo modificaciones a los programas que han sido debidamente autorizadas, siendo ellos las únicas personas autorizadas a realizar dichos cambios.
3. Verificar que todo cambio a programas cuente con los elementos necesarios para poder darle mantenimiento, es por ello la necesidad de asegurar que la documentación se encuentre debidamente actualizada.
4. Analizar la efectividad de los procedimientos de modificación de los sistemas, identificando el proceso por el cual se inician los cambios o modificaciones:

   Falla en los sistemas

   Nuevos procesos

   Actualización de Data

   Consulta de Información
5. Verificar que todo cambio realizado se realice coordinadamente entre las Áreas Usuarias y la Intendencia Nacional de Informática, a fin de que los usuarios sean informados de los cambios efectuados o de la implantación de un nuevo sistema y al mismo tiempo se realicen las coordinaciones necesarias para la capacitación y el envío de la documentación respectiva.

3.4.3 PROCEDIMIENTOS DE CONTROL DE LAS APLICACIONES

Estos procedimientos incluyen la revisión de los aplicativos más importantes, los cuales han sido descritos anteriormente. El Auditor de Sistemas debe considerar las fortalezas y debilidades para cada aplicación, con el fin de determinar las pruebas sustantivas que deberán ejecutarse.

Los usuarios de los sistemas constituyen el elemento más importante en el proceso de auditoría, debido a que ellos interactúan diariamente con los sistemas constituyéndose en los mejores evaluadores del mismo.

3.4.3.1 PROCEDIMIENTOS DEL CONTROL DEL SISTEMA DE PRINCIPALES CONTRIBUYENTES

Todas las Dependencias del interior del país cuentan con el Sistema de Principales Contribuyentes, siendo la labor del Auditor de Sistemas las siguientes:

1. Verificar que se ejecute diariamente el proceso de descarga del Sistema de RUC en Línea a Sistema de Principales Contribuyentes, a fin de tener actualizado el Directorio del Contribuyente.
2. Verificar el cumplimiento de entrega del CIR[12] , el cual contiene los datos declarados por el contribuyente y el calculado por el sistema, para cada una de las transacciones realizadas por el contribuyente, con la finalidad de evitar de que estos comprobantes sean emitidos al final de día y que no sean entregados a los contribuyentes.
3. Verificar que la transferencia de información de un contribuyente MEPECO que ha pasado a ser contribuyente PRICO, y viceversa se haya realizado de manera integra y segura.
4. Evaluar el procedimiento de carga mensual de la TIM[13] , con el propósito de verificar que se esta utilizando la tasa correcta al realizar el proceso de actualización de la deuda.
5. Verificar que se realice una buena administración de los parámetros del sistema:

---

12 Comprobantes de Información Registrada (CIR), la cual debe ser entrega al contribuyente luego de realizar una transacción.

13 Tasa de Interés Moratorio (TIM), es la tasa utilizada para el cálculo de los intereses de un tributo no pagado dentro delos plazos establecidos.

Información de los Tributos, Formularios y Dependencias

Tasas por Tributos

Calendarios de Vencimiento

En esta punto se debe tener especial cuidado de que se utilicen los parámetros correctos para las Dependencia Ubicadas en Zona de Selva y Zona de Frontera.

6. Verificar la correcta utilización de los saldos a favor y de los pagos anticipados realizados por el contribuyente.
7. Evaluar si el módulo de caja cumple con los requisitos de una caja bancaria, es decir:

   Apertura y cierre de cajas

   Refrendo de la Declaración Jurada

   Arqueo de Cajas en sus diferentes formas de pago: efectivo, cheque, documentos cancelatorios y notas de crédito.
8. Evaluar el proceso de distribución de la recaudación del día (acreditación) a los diferentes entes beneficiarios.
9. Verificar la generación de los reportes de recaudación diaria y la generación de Novedades de Recaudación para su envío a Centro de Procesamiento de la Información Central de SUNAT en Lima.
10. Verificar que se corran los procesos de Omisos a la Presentación y el proceso de Pagos Pendientes, con el fin de generar en el día las Resoluciones de Multas y las Ordenes de Pago respectivamente.
11. Verificar que el proceso de Traslado de Valores a Cobranza Coactiva se realice diariamente y el Proceso de Actualización automática de la deuda.
12. Verificar el proceso de Actualización de la Cuenta Tributaria del Contribuyente con todas las transacciones realizadas por el contribuyente.

3.4.3.2 PROCEDIMIENTOS DEL CONTROL EN EL MODULO DE CONSULTAS PRELIMINARES

En las Dependencias del interior del país sólo se utiliza el Módulo de Consultas Preliminares del Sistema de Recaudación Bancaria, debido a que el ingreso de las transacciones es realizada en los mismos bancos y centralizada en el Centro de Procesamiento de la Información Central de SUNAT, para luego distribuir las Novedades de Recaudación Bancaria a las dependencias de todo el país. Las tareas a realizar por el Auditor de Sistemas son

1. Verificar que el sistema sólo contiene información de contribuyentes MEPECOS, solicitando a la Intendencia Nacional de Informática la transferencia inmediata de la información del contribuyente en caso de que éste sea un PRICO.
2. Evaluar el Proceso de Envío de Novedades de Recaudación bancaria desde el Centro de Procesamiento de la Información Central, a fin de que se pueda contar con información actualizada.
3. Evaluar el proceso de Corrección de la Información de los pagos efectuados por el contribuyente, producto de errores en el ingreso de parte de los bancos o carga de parte de SUNAT, a fin de que se realice lo más rápido posible.
4. Revisar el proceso de integración con el Sistema de RUC en Línea, debido a que este contiene el Directorio de Contribuyentes.

3.4.3.3 PROCEDIMIENTOS DE CONTROL DEL SISTEMA DE RUC EN LÍNEA

Con la instalación de Plaza SUNAT en las diferentes dependencias del interior del país, se ha logrado la implantación de los Sistemas de RUC en Línea y el Sistema de Comprobantes de Pago. Ahora se puede decir que todas las dependencias cuentan con el este sistema, por lo que las tareas a realizar por el mismo son:

1. Revisar le procedimiento de carga de la tabla t65reduc, el cual contiene el padrón RUC reducido de todo el país, el cual ayuda a detectar la doble inscripción.
2. Evaluar el procedimiento de afectación de tributos de un contribuyente MEPECO que pasa a ser contribuyente PRICO, y viceversa, con el propósito de evitar inconsistencias en el proceso de afectación.
3. Verificar el procedimientos de Activación de RUCs de contribuyentes de otras dependencias.
4. Evaluar el Vector Fiscal Particular de los contribuyentes, a fin de evitar incongruencias debido a una mala definición del giro del negocio.
5. Revisar los procedimientos que permiten pasar a un contribuyente del Régimen General al Régimen Único Simplificado.
6. Evaluar el procedimiento de actualización en el Sistema de Comprobantes de Pago, de aquellas imprentas que han sido dadas de bajas.
7. Verificar que se realice diariamente el proceso de Envió de Novedades de RUC y el Proceso de recibir los archivos de respuestas.

3.4.3.4 PROCEDIMIENTOS DE CONTROL DEL SISTEMA DE COMPROBANTES DE PAGO

Las tareas a realizar por el Auditor de Sistemas son:

1. Verificar que se reciba diariamente el Padrón Nacional de Imprentas autorizadas para la impresión de comprobantes de pago.
2. Evaluar el procedimiento de autorización de comprobantes, con el propósito de evitar la doble facturación.

3. Revisar el procedimiento de autorización de comprobantes de pago para aquellos contribuyentes que han realizado su cambio a la dependencia donde se realiza el proceso de evaluación.

3.4.4- AUDITORIA DEL CENTRO DE PROCESAMIENTO DE LA INFORMACIÓN

El Centro de Procesamiento de la Información es el elemento más esencial con que actualmente cuentan las dependencias del interior del país, brindando un servicio muy importante tanto para los usuarios de PCs como para los usuarios de la Red UNIX, es por ello que el Auditor de Sistemas debe realizar las siguientes tareas:

1. Verificar que solamente personas autorizadas se encuentran en las instalaciones del Centro de Procesamiento de la Información y bajo la supervisión de personal del mismo.
2. Evaluar el cumplimiento de los siguientes procedimientos:

   Administración de Cuentas, el cual define las cuentas, sus funciones, los responsables de las cuentas, permisos, estándares por aplicación, procedimientos de creación y eliminación de las mismas.

   Administración de Directorios, a fin de mantener un estándar y control de los archivos que contienen.

   Administración de Procesos en Producción.

   Administración de la Transferencia de la Información, es decir controlar los archivos que transitan de un computador a otro, analizando la performance de este proceso.
3. Verificar continuamente la performance del sistema y la existencia de por lo menos 30 % de espacio libre en disco, a fin de evitar la degradación del sistema y caída del sistema.
4. Verificar que todos los Pases a Producción del Sistema de Principales Contribuyentes, Sistema de Consultas Preliminares, Sistema de RUC en

Línea y Sistema de Comprobantes de Pago en Línea se encuentren debidamente autorizados y sustentados en el formato respectivo.

5. Verificar que todas las cuentas creadas durante la implantación de los sistemas se encuentren debidamente autorizadas y sustentadas en el formato respectivo. Aquí el Auditor de Sistemas debe verificar que exista una cuenta por usuario, evitando de esta manera que el usuario comparta su cuenta.
6. Revisar la documentación existente a fin de verificar que se cuenta con los Manuales del Sistema Operativo, Manuales del Administrador de la Base de Datos, Manuales de los Sistemas y Documentación relativa a los Procesos que se realizan.
7. Verificar que se realizan diariamente los procesos de BackUp de nivel 1 (Backups increméntales), los procesos semanales de BackUp de nivel 0 (Backups totales) y los procesos mensuales de BackUp de nivel 0 (Backups histórico), de las Bases de Datos y de los On-Lines de los sistemas.
8. Verificar el procedimiento de control (inventario y contenido de las cintas) y seguridad de la información: Backups de nivel 1 en el Centro de Procesamiento de la Información, BackUp de nivel 0 en un lugar seguro fuera del Centro de Procesamiento de la Información y BackUp histórico es remitido a Lima para su custodia definitiva. En esta etapa es necesario realizar una prueba de los Backups, a fin de asegurar que se ha realizado correctamente.
9. Evaluar el nivel de respuesta del personal a los problemas presentados con las Aplicaciones, con el Sistema Operativo, Software de Aplicación para PCs y coordinación con la Sede Central de los problemas que no pueden ser resueltos. Esto nos va a garantizar que existan problemas sin solución, los cuales pueden ser causantes de la pérdida de la operatividad funcional.

10. Verificar que exista una adecuada distribución de PCs y Notebooks, o en su defecto realizar las coordinaciones con el Departamento de Soporte Técnico, a fin de que se asigne más equipos a la Intendencia Regional u Oficina Zonal.
11. Realizar un análisis de la Red de Datos actual, con el propósito de asegurar de que cubra todas las áreas operativas, y en caso de que no cuenten con ellas recomendar que se amplíe la red o se habiliten más salidas.
12. Verificar la existencia y cumplimiento del cronograma de mantenimiento y reparación de equipos computacionales, con el propósito de minimizar las fallas de los equipos y reducir el número de equipos que se envían a Lima para su reparación. Además es necesario realizar un análisis del tiempo de reparación de los equipos, a fin de evaluar el nivel de cumplimiento de los proveedores de este servicio.
13. Verificar la existencia de copias autorizadas de Software de Usuario Final y de Antivirus, a fin de brindar un mejor servicio a los usuarios.
14. Verificar el proceso de transmisión de las novedades de recaudación desde las Dependencias Descentralizadas de SUNAT al Sistema Central, teniendo en cuenta:
    - La encriptación de la información a ser transmitida
    - La confirmación del proceso de recepción de la información.

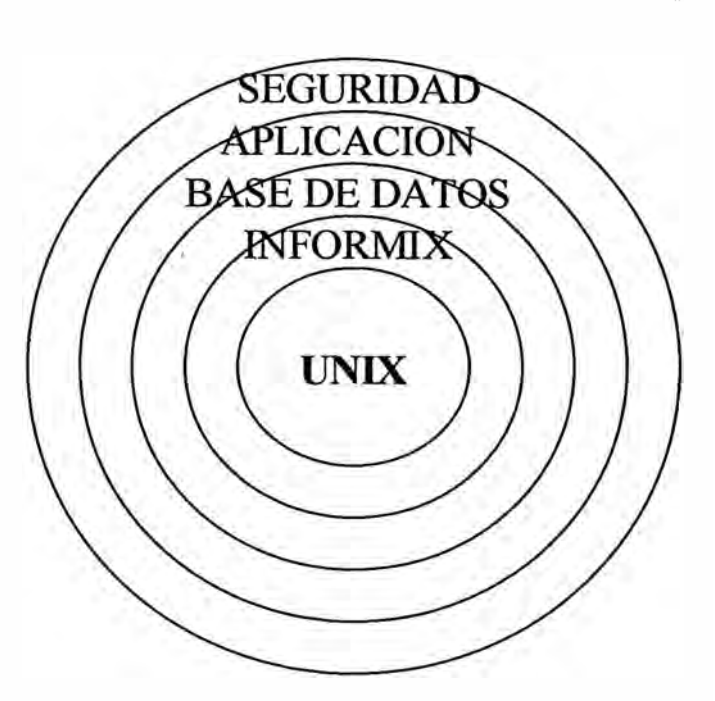
3.4.5 AUDITORIA DEL PROCESO DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos a lograr por el Auditor de Sistemas en este proceso de auditoría son:

- Mantener un nivel de performance en los procesos en tiempo real
- Brindar un sistema de emergencia en casos de caídas del servidor de atención al público.
- Brindar al usuario la seguridad de que la B.D. conserva la integridad de la información.

Para ello la SUNAT utiliza niveles de seguridad que van desde el Sistema Operativo hasta la Seguridad Física del ambiente de procesamiento de datos con la finalidad de reducir la probabilidad de riesgos.

Figura 3.6 : Niveles de Seguridad



Los tareas a realizar por el Auditor de Sistemas son:

1. Verificar el acceso de los contribuyentes a las dependencias de SUNAT, restringiendo el acceso sólo a áreas autorizadas.
2. Determinar si la ubicación y tamaño del Centro de Procesamiento de la Información es el más seguro y adecuado dentro de la dependencia.
3. Evaluar la seguridad física del Centro de Procesamiento de la Información, restringiendo el acceso solamente a personas autorizadas o a la realización de visitas bajo supervisión de personal del mismo.

4. Verificar si se cuenta con un sistema de seguridad contra incendios, y lo más importante aún asegurarse de que funcionen. En esta parte es necesario determinar si el personal del Centro de Procesamiento de la Información tiene conocimiento de la práctica contraincendios y el manejo de los diferentes dispositivos que se usa.
5. Evaluar si el Centro de Procesamiento de la Información requiere de un sistema de aire acondicionado y si cuenta con los dispositivos necesarios para medir la temperatura y humedad.
6. Verificar que las cuentas asignadas a los usuarios tengan passwords triviales o en su defecto no cuenten con un password de seguridad que limite el acceso a los equipos de cómputo. Además es necesario verificar que las cuentas de usuarios que ya no laboran en la dependencia sean reasignadas o anuladas, comprobando que se encuentren sustentadas en el formato respectivo.
7. Revisar el estado en que se encuentran el UPS y el Grupo Electrógeno, verificando su operatividad y capacidad, a fin abarcar a todas las áreas usuarias que utilizan equipos de cómputo. Es necesario evaluar la ubicación actual de los mismos con el propósito de asegurar su operatividad.

   Revisión de las políticas, procedimientos y prácticas para evitar interrupciones prolongadas del servicio de procesamiento de datos
8. Verificar la existencia de seguros que permitan cubrir el costos de restablecer las operaciones.
9. Evaluar el proceso de asignación de cuentas, mediante:

   Procedimientos de administración de usuarios

   Cambios periódicos de Passwords

   Control de intentos de acceso no autorizados

10. Controlar el envío diario de las cintas a un lugar seguro dentro de la dependencia (bóvedas) y el envío semanal a un lugar externo como medidas de prevención.

CONCLUSIONES

1. La información es el activo más importante de SUNAT, el cual es muy importante para el progreso y desarrollo de la institución, siendo necesario priorizar las características del mismo:

   Confidenciabilidad que la información sea divulgada sólo a los usuarios autorizados.

   Integridad : que la información sólo sea modificada por personal autorizado.

   Disponibilidad : que la información sea utilizada cuándo y cómo el usuario lo requiera.

   La integridad y confiabilidad de las transacciones constituyen un requisito fundamental para la toma de decisiones, pudiendo representar para SUNAT perjuicios de orden económico y de desarrollo institucional si no se cuenta con información confiable y exacta.

2. La auditoría es un proceso continuo, siendo necesario realizar un seguimiento a fin de determinar si se han tomado las acciones correctivas correspondientes de acuerdo a las recomendaciones de auditoría. Para ello se realiza un proceso de retroalimentación periódica a fin de actualizar el estado de las observaciones, por medio de informes trimestrales que se solicitan al personal del Centro de Procesamiento de la Información.

3. Un Proceso de Auditoría no es posible llevarse a cabo si no se cuenta con la aprobación y respaldo de las Gerencia de la Intendencia Nacional de Informática y del Intendente Regional o Jefe Zonal. Esto es un factor determinante para el Proceso de Auditoría, debido a que involucra a todos los servicios y niveles dentro de la Dependencia.

4. Solamente implementando medidas de seguridad que permitan proteger los activos de información se puede reducir la probabilidad del riesgo a acciones no autorizadas que amenacen la integridad de la información.

5. La protección de los activos de SUNAT son vitales, debido a que la misma tiene como objetivo dotar al estado de los recursos le son necesarios. La falta de operatividad del Centro de Procesamiento de la Información, puede convertirse fácilmente en una disminución de los niveles de recaudación.

6. El Proceso de Auditoría presentada en este informe, es un proceso netamente preventivo, debido a que va a permitir identificar y solucionar los problemas potenciales antes de que se conviertan en pérdidas.

7. El cumplimiento de los procedimientos administrativos no es posible, si no se realizan Procesos de Auditorías periódicos.

8. La SUNAT por ser un organismo recaudador de impuesto, se encuentra permanentemente expuesta a riesgos, siendo necesario establecer mecanismos de prevención y detección de fraudes.

RECOMENDACIONES

1. Definir las responsabilidades de los empleados, y el papel que desempeñan los mismos en al protección de la información, estableciendo sanciones en el caso de incurrir en negligencias.

2. Realizar el Proceso de Auditoría a los Centro de Procesamiento de la Información del Interior del País por lo menos una vez al año, debido a que esto nos va a permitir descubrir nuestras debilidades y coordinar con las áreas involucradas en la solución de las mismas.

3. Realizar el seguimiento a cada uno de las observaciones encontradas, hasta llegar a una solución definitiva. Un Proceso de Auditoría no tiene efecto si es que las recomendaciones sugeridas no son implantadas.

4. Revisar periódicamente las normas, políticas y procedimientos de la institución, debido a la innovación tecnológica, la cual deja absoleta a muchos de ellos.

5. Orientar al personal involucrado en el Proceso de Auditoría que la labor realizada por el Auditor de Sistemas no es evaluar su trabajo, sino por el contrario es ayudar a descubrir errores y recomendar soluciones para los mismos antes de que se convierta en una pérdida financiera para la institución.

6. Tomar siempre en cuenta las observaciones presentadas por los usuarios, debido a que son éstos los que diariamente interactúan con los sistemas, conociendo las debilidades y fortalezas de los mismos.

BIBLIOGRAFÍA

- APCI - William Molina Ore, Auditoria Efectiva del Area de Sistemas, Lima, Julio de 1995.
- CISA. Manual de Revisión CISA EDPAA. 1993.
- Echenique García, José Antonio. Auditoría en Informática. Lima, 1995.
- IBM del Perú- Fernando Salmeron, Plan de Contingencia y Recuperación en Caso de Desastre, Lima, Setiembre de 1994.
- IBM del Perú- Fernando Salmeron, Auditoría de Sistemas de Información y de Aplicaciones, Lima, Diciembre de 1994.
- IBM del Perú- Fernando Salmeron, Seguridad y Control de la Información, Lima,Enero de 1995.
- INEI, Auditoría de Sistemas, Lima, Abril de 1996.
- INEI, Curso de Protección Contra Virus Informático y Seguridad de la Información, Lima, Mayo de 1996.
- FINE, Leonard. Seguridad en Centros de Cómputo: Políticas y Procedimientos. Primera Edición. Editorial Trillas S.A. México, 1990.
- LI, David H. Auditoría en Centros de Cómputo: Objetivos, Lineamientos y Procedimientos. Primera Edición. Editorial Trillas S.A. México, 1990.
- SUAREZ, Andres S. La Auditoría Moderna, Un Análisis Conceptual y Metodológico. Primera Edición. Editorial Mc Graw Hill, Interamericana de España S.A. Madrid, 1991.
- WATNE, Donald y TURNEY, Peter . Auditing EDP Systems. Second Edition. USA, 1990.

- MURPHY, Michael A. y PARKER, Xenia L. Handbook of EDP Auditing. Second Edition. Warren, Gorham & Lamont. Boston, New York, 1990.
- SFOGLIA, Peter. SysBase Security. Tomado de The EDP Auditor Journal, 1993. Vol II.
- WILLIANS, Paul y CANGEMI, Michael. Microcomputer - Based Audit Tools. Tomado de The EDP Auditor Journal, 1990. Vol IV.

ANEXOS

ANEXO 1 : METODOLOGÍA DE ANÁLISIS DE RIESGOS

El grupo de Análisis de Riesgos es multidisciplinario, que requiere la participación de una variedad de personas con una amplitud de conocimientos. Dicho grupo, debe estar conformado por :

- ***Arreas usuarias***, los cuales van a determinar los riesgos correspondientes a sus áreas,
- ***Personal de Procesamiento de Datos,***
- ***Auditores,***
- ***Personal de Seguridad***, quienes van a determinar los riesgos inherentes a la seguridad fisica, y
- ***Consultores Externos***, quienes pueden brindar asesoramiento en temas específicos.

1. IDENTIFICACIÓN DE RIESGOS

Es el primer paso del Análisis de Riesgos, el cual consiste en determinar a que riesgos esta expuesta la información. Los riesgos están clasificados en tres grupos:

- ***Destrucción***, que implica pérdida de datos.
- ***Modificación***, que implica que los datos son cambiados sin autorización.
- ***Divulgación***, que implica la diseminación de los datos fuera de los límites autorizados.

Cada uno de estos grupos puede estar dividido en Accidental e Intencional, dependiendo de la forma en que ocurra el evento.

1.1 CAUSAS DE LOS RIESGOS

Es necesario identificar las causas de los riesgos, aunque muchas veces un riesgo puede tener múltiples causas, y en otros casos, una causa puede causar múltiples riesgos.

La lista que a continuación se presenta indica algunas de las causas de destrucción:

- ***Fallas*** : suministros, servicios, etc.
- ***Intrusos*** : casual, malicioso, etc.
- ***Desastres Naturales***: fuego, inundaciones y tormentas, terremotos, etc.
- ***Desastres Humanos*** : accidentes, vandalismo y terrorismo.
- ***Errores y Omisiones*** : en los programas o datos.
- ***Deshonestidad y Malicia*** : del personal de informática, de los usuarios o de terceros.

1.2 PUNTOS DE RIESGO

Los puntos de riesgo están diseminados a lo largo de todo el flujo de datos de la organización, desde el momento en que son originados hasta su deshecho por parte del usuario. Los puntos de riesgo incluyen:

- Preparación de entradas
- Transporte
- Conversión
- Transmisión
- Recibo en el procesamiento de la información
- Procesamiento
- Preparación de salidas
- Distribución de salidas
- Uso de la información por los usuarios
- Eliminación de la información.

2. DETERMINACIÓN DE MEDIDAS DE SEGURIDAD

Después de identificar los riesgos es necesario determinar que controles o medidas de seguridad van a ser implementadas a fin de evitar o reducir la posibilidad de ocurrencia de un riesgo o minimizar su impacto. Para ello es necesario implementar medidas de seguridad:

- ***Preventivas***, diseñados para evitar que se produzca un error, a fin de eliminar o reducir la probabilidad de los mismos.
- ***Correctivas***, son aquellos que corrigen los errores, omisiones o actos maliciosos una vez detectados.
- ***Detectivas***, que detectan que se ha producido un error.

3. EVALUACIÓN FINANCIERA DE RIESGOS

Evalúa el impacto que la ocurrencia de cada uno de los riesgos determinados puede producir en la organización. El costo de un riesgo es el resultado de dos factores:

- Impacto Financiero
- Probabilidad de Ocurrencia

Sin embargo, el costo de un riesgo es muchas veces muy difícil de determinar, debido a que pueden ser intangibles, como por ejemplo la imagen empresarial.

La evaluación financiera de un riesgo se puede determinar usando alguno de los siguientes métodos:

a) **Cálculo Directo :** Cuando se determina usando la experiencia e información estadística propia.

b) **Estimación :** Consiste en utilizar la mejor estimación para asignar valores al impacto y a la probabilidad.

c) **Medidas Menos Costosas Primero :** Este enfoque requiere bajo presupuesto, por lo que puede ser implementada en una organización pequeña, pudiéndose implementar una buena cantidad de medidas de seguridad a fin de reducir múltiples riesgos.

d) **Riesgos más Costosos Primero :** Son riesgos que derivan de errores y omisiones, requiriendo también medidas costosas para combatirlo. Se requieren técnicas de administración de sistemas para minimizar su efecto.

Para la reducción de un riesgo en particular se puede requerir de múltiples medidas.

e) **Mejor Relación Costo/Beneficio :** Permite evaluar las distintas medidas y tomar una decisión en base a su relación costo beneficio.

Análisis de Costo/Beneficio		***Medidas Propuestas***				
		Medida A	***Medida B***	***Medida C***	***Medida D***	***Medida E***
Riesgos	***Costos***	***500***	***1500***	***150***	***4500***	***200***
1	**1000**	15 % 150		70 % 700		
2	**10000**				90 % 9000	
3	**5000**		30 % 1500			30 % 1500
4	**4000**		50 % 2000			
Contribución		-350	2000	550	4500	-500

4. DETERMINACIÓN DE COSTO Y EFECTIVIDAD DE MEDIDAS

Determinar el costo de las medidas de seguridad es más fácil que evaluar el riesgo, debido a que se relacionan con dispositivos físicos, programas, tiempo de computación, etc. Se puede usar también la estimación en caso de no contar con datos para determinar el costo.

Determinar la efectividad es el porcentaje en que cada medida puede reducir el riesgo. No es tan fácil como determinar el costo. En algunos casos el cálculo puede resultar bastante aproximado, pero en otros casos puede llevar a un amplio rango de porcentajes.

5. EVALUACIÓN GERENCIAL

Deben decidirse a que medidas combaten que riesgo, y qué medidas serán aplicadas, a fin de diseñar un plan de implementación. La gerencia toma decisiones en base a:

- Estrategias
- Imagen Empresarial
- Prioridades
- Política
- Relaciones con clientes o proveedores
- Relaciones con organismos del gobierno.

Se requiere un plan para implementar distintas medidas, de tal forma que los objetivos gerenciales sean logrados.

ANEXO 2 : TÉCNICAS DE RECOPILACIÓN DE EVIDENCIA

La evidencia es un prueba clave en el proceso de auditoría, es por ello que el auditor debe tener conocimiento de como obtenerla y examinarla, con el propósito de respaldar los hallazgos de auditoría.

1. REVISION DE ESTRUCTURAS ORGANIZACIONALES

El auditor de Sistemas de Información debe estar en condiciones de revisar estructuras organizacionales y evaluar sus controles organizativos generales.

2. REVISION DE NORMAS DE DOCUMENTACION DE SISTEMAS

Un primer paso para revisar la documentación de un sistema de información, es comprender las normas vigentes sobre documentación dentro de la organización. Se debe buscar un nivel mínimo de documentación el cual debe incluir:

- Documentos que inician el desarrollo de sistemas,
- Especificaciones de diseño funcional,
- Historia de cambios a los programas, y
- Manuales de documentación de usuarios.

El auditor de Sistemas de Información debe estar en condiciones de revisar la documentación de los sistemas y ver si cumple con las normas de documentación de la organización.

3. ENTREVISTAS CON EL PERSONAL APROPIADO

La entrevistas de auditoría, es una destreza importante de los auditores de Sistemas de Información. Las entrevistas se organizan de antemano y siguen un esquema fijo, con

algunas notas de las entrevistas. Un buen enfoque es un formulario de entrevista preparado.

El propósito de la entrevista es para recopilar evidencia de auditoría, siendo de naturaleza de descubrimiento y no acusatoria.

4. OBSERVACION DE OPERACIONES Y ACTUACION DE LOS EMPLEADOS

La observación de operaciones es una técnica de auditoría clave para muchos tipos de revisiones. El auditor de Sistemas de Información debe ser prudente al realizar sus observaciones y documentarlo detalladamente a finde presentarlo como evidencia de auditoría, si así se requiere.

5. TECNICAS DE DOCUMENTACION DE AUDITORIA

El auditor de Sistemas de Información debe poseer técnicas para documentar un sistema de información, así como para documentar el ambiente del sistema de información.

6. SELECCION Y PRUEBA DE CONTROLES CLAVES

El auditor de Sistemas de Información debe identificar los controles claves de aplicaciones, a fin de identificar los puntos de control claves en las aplicaciones. Esto le va a permitir lograr una comprensión preliminar por medio de las pruebas de cumplimiento de dichos controles, a fin de determinar si funcionan como deben.

7. APLICACION DE TECNICAS DE MUESTREO

El auditor de Sistemas de Información debe tener una comprensión cabal de las técnicas de muestreo, a fin de aplicar el tipo adecuado de pruebas.