AUDITORÍA INFORMÁTICA PARA SEVICOL LTDA

ALDEMAR SILVA MALDONADO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS FÍSICO-MECÁNICAS
ESCUELA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
BUCARAMANGA
2004

AUDITORÍA INFORMÁTICA PARA SEVICOL LTDA

ALDEMAR SILVA MALDONADO

Proyecto de grado para optar al título de
Ingeniero de Sistemas.

Director:
Ing. José Cárcamo Sepúlveda

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS FÍSICO-MECÁNICAS
ESCUELA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
BUCARAMANGA
2004

Nota de aceptación

Proyecto de Grado

_____

Aprobado

_____

Nota: 4.5

_____

_____

Director

Ing. José Cárcamo Sepúlveda

_____

Jurado

Ing. Hugo Hernando Andrade Sosa

_____

Jurado

Ing. Alfonso Mendoza Castellanos

AGRADECIMIENTOS

El autor expresa sus agradecimientos a:

La UNIVERSIDAD INDUSTRIAL DE SANTANDER por el aporte en nuestra formación profesional y personal.

SEVICOL LTDA., por la confianza depositada en el autor del presente proyecto.

Ingeniero José Cárcamo Sepúlveda por su colaboración y apoyo como director.

Ingeniero Luis Carlos Gómez Florez por su orientación en el inicio del proyecto.

A los ingenieros Nicolás Leuro y William Tristancho por su ayuda incondicional.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

TITULO
AUDITORÍA INFORMÁTICA PARA SEVICOL LTDA.*

AUTOR
Silva Maldonado, Aldemar**

PALABRAS CLAVES: Auditoría Informática, Riesgo, Requerimientos Fiduciarios, COBIT, Control Interno Informático.

DESCRIPCIÓN

El presente proyecto describe el desarrollo de una auditoría informática siguiendo los requerimientos fiduciarios y de seguridad expuestos en el modelo COBIT, orientado por el estudio de riesgos y diseño de controles y de esta manera contribuir a la definición de un sistema de control interno informático que administre eficientemente el recurso informático de una organización empresarial.

Como forma de lograr los objetivos se define una metodología que guié el proceso, iniciando con una etapa preliminar que nos permite conocer la organización empresarial y su recurso tecnológico (Datos, Aplicaciones, Instalaciones, Personas, Tecnologías), continuando con el estudio de riesgos donde se definen, identifican, valoran y jerarquizan los riesgos presentes en el entorno informático; siguiendo con la etapa de elaboración y ejecución de pruebas que verifican y evidencian el grado de peligrosidad de los riesgos identificados; posteriormente en la etapa de diseño de controles se definen y documentan los controles que contrarrestaran los efectos de los riesgos presentes en el entorno informático de la empresa; finalmente en la etapa de implementación se documentan las recomendaciones correspondientes al resultado de las etapas anteriores además, se incluye el diseño del sistema de control interno informático donde se definen las políticas y normas que gobernarán el entorno informático en un marco de cuatro dominios (Organización general del servicio, desarrollo y mantenimiento de software, entorno de producción, funciones de asistencia técnica y seguridad de datos), definidos para un marco aceptado de administración eficiente de este recurso.

Este trabajo se muestra también como un caso de estudio particular a una empresa del sector de las pymes.

---

* Proyecto de grado en la modalidad de práctica empresarial
** Facultad de Ingenierías Físico-Mecánicas, Ingeniería de Sistemas e Informática
Director del proyecto: José Cárcamo Sepúlveda

ABSTRACT

TITLE
INFORMATION TECHNOLOGY (IT) AUDIT FOR SEVICOL LTD.*

AUTHOR
Silva Maldonado, Aldemar**

KEYWORDS: IT AUDIT, RISK, INFORMATION REQUIREMENTS, COBIT, INTERNAL CONTROL SYSTEM

DESCRIPTION

This project covers an auditing process which meets the security and fiduciary requirements stated in the COBIT model which is based on risk studies and control design letting the enterprise build its internal control system..

In order to archive the objectives proposed a methodology is defined which directs the process which begins with a preliminary stage which let us to know the organization and its I.T. resources (Data, Applications, Facilities, People, Technology), following by the risk study where they are defined, identified, assessed and ---- within the I.T. context. In the testing making and execution stage the potential damage of each risk is identified. Next int the control design stage the controls which fight the effects of the risk are defined and documented; endlessly, in the implementation stage it is documenting the concern advice to the result in the previous stages, moreover, it is included the design of the internal control system, where it is defined the politicians and norms that will govern the IT resources in a frame of four domains (Service general organization, Development and maintain of software, Production and Technical assistance functions and Data security) defined for good practices for effective management of information and related information technology.

This work is an example of how to develop the previous methodology in a company of the pymes sector.

* Degree project in the modality of enterprise practice
** Faculty of Physical – Mechanical Engineerings. Systems and Computer Engineering.
Director of the project: José Cárcamo Sepúlveda

INTRODUCCIÓN

El ambiente organizacional que podemos encontrar en algunas empresas esta marcado por un número determinado de procesos y actividades que raras veces actúan de forma integral, y cuando parece que lo hacen es demasiado el tiempo necesario verificando su funcionalidad. Afortunadamente estas mismas empresas cuentan con un recurso informático bastante útil los sistemas de información, herramientas capaces de llevar en forma integral los procesos administrativos y operativos de las empresas, herramientas que le permiten a los empresarios muchas veces poco conocedores de informática verificar, controlar y administrar la información de su empresa. Esta capacidad que presentan los sistemas de información da como resultado una excesiva confianza sobre los mismos y es poco el control y seguimiento que se le hacen para verificar su funcionalidad generando quejas y reclamos que comienzan a despertar la idea que algo no esta funcionando correctamente.

La Auditoría Informática se presenta como un servicio que ayuda a valorar la eficacia y eficiencia del entorno informático de una empresa. Además, contribuye a generar una cultura de administración de este recurso.

El presente informe de AUDITORIA INFORMATICA EN SEVICOL LTDA, muestra en su primer capitulo la descripción de la empresa y el planteamiento de su problema, el segundo capitulo los fundamentos necesarios para comprender la MISIÓN de un trabajo de auditoria, el tercer capitulo la metodología utilizada y por último el cuarto capitulo el desarrollo del trabajo aplicando el método anterior y la entrega de las recomendaciones objetivo final de este trabajo.

1. PRESENTACIÓN DEL PROYECTO

1.1 ANTECEDENTES

1.1.1 PRESENTACIÓN DE SEVICOL LTDA.

El 11 de abril de 1973, ante la notaría primera de Bucaramanga, se constituyó la empresa de SEGURIDAD Y VIGILANCIA COLOMBIANA, "SEVICOL LTDA", dando así inicio a una de las más importantes empresas de Santander para Colombia.
La consolidación de SEVICOL LTDA se fundamenta en una infraestructura que cuenta con los mejores soportes en cuanto a personal calificado, patrullas de reacción inmediata y equipos de telecomunicaciones.

Con domicilio principal en la ciudad de Bucaramanga, y agencias en las ciudades de Bogotá, Cúcuta, Villavicencio, Barrancabermeja y puestos en Arauca, San Gil, Socorro, Vélez, Ocaña, Pamplona, El Centro Puerto Wilches, Puerto Berrío, Sabana de Torres y Aguachica.

1.1.2 MISIÓN

Ser la empresa excelente en la presentación del servicio de Seguridad en el ámbito nacional, con un alto grado de pertenencia, eficiencia, utilidad y rentabilidad, por nuestros clientes, la empresa, nuestros empleados y el fortalecimiento del gremio.

SEVICOL LTDA, es una empresa privada, que ofrece sus servicios de Vigilancia y Seguridad Fija, Móvil y Electrónica en Colombia, buscando la mayor cobertura posible en forma competitiva, eficiente y cumpliendo con todos los requisitos de Ley. Fundada con objetivos básicos de rentabilidad, permanencia y alto compromiso social con generación de empleo y estabilidad laboral, procurando siempre un clima de trabajo de respeto mutuo y oportunidades de desarrollo, contribuyendo al progreso nacional.

1.1.3 VISIÓN

SEVICOL LTDA. Será percibida por la Sociedad, el Estado y los Clientes, como una de las mejores empresas de servicios de seguridad privada. Integrante de un sector económico conformado por verdaderos profesionales, tecnológicamente desarrollado y soporte esencial de seguridad ciudadana.

SEVICOL LTDA, se proyecta como una empresa líder en la prestación de Servicios Integrales de Seguridad en el ramo Residencial, Industrial, Comercial y Financiero de carácter público o privado, aplicando la tecnología a su alcance, profesionalizando a sus empleados, diseñando y desarrollando nuevos servicios. Su infraestructura se mantendrá a la vanguardia con el fin de obtener procesos operativos y administrativos

ágiles y versátiles para cubrir cualquier necesidad de sus clientes y llegar a consolidarse como modelo social, velando por la Seguridad ciudadana.

1.1.4 PORTAFOLIO DE SERVICIOS

SEVICOL LTDA cuenta con el personal mejor calificado y de más alto nivel de seguridad en la implementación del Sistema Integral de Seguridad Preventiva SISP, para prestar los servicios de:

- Vigilancia fija y móvil
- Vigilancia Bancaria
- Vigilancia Comercial
- Vigilancia Industrial
- Vigilancia Residencial
- Vigilancia Especializada a personas
- Escolta a Vehículos y mercancías
- Monitoreo de alarmas con Reacción inmediata[1].

1.1.5 EVOLUCIÓN TECNOLOGICA EN SEVICOL LTDA.

Uno de los principios básicos de las entidades privadas es impulsar el desarrollo socioeconómico de las personas vinculadas, mediante el aprovechamiento de los recursos que se dispone.

[1] [1] Portafolio de Servicios SEVICOL LTDA. Bucaramanga, marzo de 2002

Sin embargo, la ejecución de los planes y programas pueden verse alterados, si quienes tienen la responsabilidad de tomar decisiones no disponen de sistemas de información que determinen el avance y comportamiento de los programas y los resultados reales obtenidos.

A partir de 1983 se inicio un proceso de apoyo a la gestión administrativa mediante la sistematización de la contabilidad con un service de las operaciones contables con una firma de la ciudad, pero las limitaciones tecnológicas del equipo de esa firma llevó a la empresa a adquirir un sistema de contabilidad desarrollado en Basic el cual corría en un Microprocesador Radio Schack modelo 12 con edición de listados en una impresora Star modelo 1000.

Debido al crecimiento de las operaciones de vigilancia la empresa decidió confiar a dos egresados de la Universidad Industrial de Santander el desarrollo de un sistema de información para el control de los registros laborales y financieros.

Fue así, que en el año de 1990 a partir de las necesidades antes mencionadas que SEVICOL LTDA., pacto realizar en convenio con la UNIVERSIDAD INDUSTRIAL DE SANTANDER un sistema de información, que reemplace y optimice los procesos manuales y automatizados que se venían realizando en los departamentos de personal y contabilidad y dar solución a los inconvenientes que se venían presentando tales como:

- El tener que esperar hasta el final de mes, para la consolidación de las novedades de los empleados, hacia que el proceso de liquidación fuera demorado.
- La elaboración de cheques para todos los empleados, era un proceso largo y con riesgo de errores, además de ser costoso para la empresa.
- Era muy tedioso preparar informes a los entes fiscalizadores, puesto que había que hacer manualmente una relación del personal vinculado y sus respectivas novedades de inclusiones y retiros.
- El sistema de nómina no permitía la liquidación de prestaciones sociales, ocasionando trabajo manual a los departamentos de personal y contabilidad.
- El sistema de contabilidad no estaba en capacidad de presentar estados financieros, dejando a la gerencia sin herramientas para evaluar la empresa.
- La elaboración manual de los comprobantes de caja y egreso y notas de contabilidad hacían lento el proceso de contabilización de los registros de la empresa, ocasionando retrasos.

De esta forma el nuevo proyecto de sistemas tenia como prioridad dar respuesta a los problemas antes planteados lo que dio como resultado la definición de los siguientes objetivos para el nuevo sistema de información:

1. Desarrollar un Sub-sistema de Personal que permita un control sobre: la admisión de aspirantes, el registro de personal, la edición de las nóminas, la

liquidación de los beneficios sociales y la edición de reportes para el control de las entidades encargadas de la vigilancia de ésta actividad.

2. Implementar un Sub-sistema Financiero con el fin de ejercer un seguimiento a las operaciones de la empresa y determinar objetivamente el estado de las mismas, mediante informes como: Balance General, estado de Perdidas y Ganancias, Índices Financieros e Informes Tributarios.
3. Enlazar los Sub-sistemas permitiendo al usuario la utilización y el proceso de la información de una forma fácil y sencilla y a mismo tiempo evitando la duplicidad en los datos

Análogamente, se identifico el recurso tecnológico necesario para poder llevar a cabo la implementación del proyecto así:

- **Soporte Lógico**: El sistema fue desarrollado en un administrador de base de datos de cuarta generación llamado DataEase, implementado en un ambiente monousuario bajo el sistema operacional DOS, pudiéndose llevar a un ambiente multiusuario utilizando redes de comunicación. Cabe destacarse que DataEase es una base de datos relacional que permite administrar sistemas distribuidos de información.
- **Procesamiento**: Procesamiento en línea, al capturar los datos de los documentos fuentes se utiliza el procesamiento en línea, que permite verificar simultáneamente la información.

- **Procesamiento en batch:** Debido al tipo de información que sé esta manipulando, se hace necesario la validación total de la información, para asignar responsabilidad a un funcionario; quien después de verificar la grabación autoriza la continuación de los procesos en batch.
- **Soporte Físico:** Los requerimientos mínimos eran:
  - Un microcomputador con procesador 80286, velocidad de procesamiento 12 MHZ, memoria principal 640 Kb, disco duro 40 MB, unidad de disquete de 5 ¼", teclado, puertos seriales y paralelos y una impresora de carro ancho[2].

Luego de esta etapa de conocimiento e identificación de necesidades y recursos y de un trabajo organizado y planeado por parte de los ingenieros responsables se entrega formalmente el sistema de información probado con registros históricos de los movimientos de 1990 con todos los reportes necesarios para e análisis financiero, permitiendo generar además la información laboral y tributaria exigidas por las reformas de 1990.

Además, los informes que genera el sistema cumplen con las exigencias de los crecientes reportes periódicos requeridos por las entidades competentes.

[2] PATIÑO OROZCO, Juan Carlos y RUEDA RINCON, Carlos Arturo, Sistema de Administración de los Recursos Humanos y Operativos para una Empresa de Vigilancia Privada, Tesis de Grado, UIS 1991

1.1.6 ORIGEN DE LA SITUACIÓN PROBLEMA

Este crecimiento tanto en las operaciones como en el número de programas ofrecidos ha ocasionado un importante impacto. La información pasa a ser un activo fundamental, y la necesidad de que esta información estuviera disponible en el momento oportuno y con un alto grado de confiabilidad que permite confiar en ella, se hace cada vez más esencial. Por esta razón la Empresa ha invertido dinero en la adquisición de tecnología traducida en software y hardware para automatizar y optimizar los procesos más reiterativos e importantes, así como en personal capacitado para realizar los desarrollos informáticos internos que fueran necesarios.

Sin embargo, y a pesar de los avances alcanzados, se ha podido observar una serie de eventos que pueden poner en riesgo la Empresa tales como:

1. SEVICOL cuenta con una RED NOVEL 4.0 y aunque los equipos de todas las dependencias se encuentran conectados a la red, es poco el uso que se le da a esta herramienta, además no cuenta con las suficientes características de seguridad permitiendo que cualquier persona pueda si quiere causar algún daño.
2. No se cuenta con la respectiva DOCUMENTACION de las diferentes aplicaciones de producción de información.
3. Desde el punto de vista de PROCESO ADMINISTRATIVO (Planeación, Organización, Dirección, y Control), del entorno informático es muy

deficiente. Es decir, las mejoras o arreglos se van dando en la marcha a medida que surge la necesidad y no por un debido proceso administrativo. Además, el encargado de la función informática en la empresa es a su vez responsable de otras actividades lo que en ocasiones repercute negativamente en su buen desempeño como jefe de sistemas.

4. No existe un PLAN DE CONTINGENCIAS que les permita superar acontecimientos que atenten contra el buen funcionamiento de la función informática.
5. Perdida total de datos ingresados en un periodo en la Aplicación Nomina por interrupción eléctrica.
6. Acepta registro de operaciones contables en periodos inexistentes, es decir, tiene deficiencias en la validación de datos.

De tal forma que se hace necesario fortalecer el Entorno Informático de Sevicol, con el fin de garantizar la perennidad del mismo y optimizar el uso de los recursos que actualmente posee, mediante un proceso de AUDITORIA, que permitirá emitir una opinión profesional sobre la eficacia y eficiencia del Entorno Informático de Sevicol Ltda.

1.2 OBJETIVOS

1.2.1 OBJETIVO GENERAL

Realizar una Auditoria Informática para SEVICOL LTDA., mediante el estudio de riesgos y diseño de controles según los requerimientos fiduciarios y de seguridad del modelo COBIT[3] 3ra. Edición y contribuir a la implantación del sistema de control interno informático de la compañía.

1.2.2 Objetivos Específicos

a) Elaborar un estudio para documentar la configuración del sistema que contenga

- Detalles de la red, esquema de la red, descripción de la configuración de hardware de comunicaciones, descripción del software que se utiliza, control de la red y consideraciones relativas a la seguridad de la red, flujos de información, número de puestos de trabajo, número de personas por puesto de trabajo, niveles de control y demás elementos relacionados.

b) Para la implantación del sistema de control interno informático habrá que definir:

[3] ISACA: Information Systems Audit and Control Foundation, COBIT Objetivos de Control, 3ra Edición Julio de 2000

- Gestión de sistemas de información: políticas, pautas y normas técnicas que sirvan de base para el diseño y la implantación de los sistemas de información y de los controles correspondientes.

- Administración de sistemas: controles sobre la actividad de los centros de datos y otras funciones de apoyo al sistema, incluyendo la administración de las redes.

- Seguridad: incluye las tres clases de controles fundamentales implantados en el Software y Hardware del sistema, integridad del sistema, confidencialidad (control de acceso) y disponibilidad.

c) Estudio de riesgos informáticos: Definición de los riesgos presentes en cada uno de los procesos según los requerimientos fiduciarios y de seguridad del modelo COBIT 3ra. Edición.

d) Definición de Controles

- Elaboración del diseño o re-diseño de controles preventivos, detectivos y correctivos que tengan lugar en el S.I.

- Implementación de los controles en la aplicación base del S.I, utilizando la herramienta de desarrollo DataEase V.4.0.

1.3 JUSTIFICACIÓN

Desde hace muchos años nuestro país cuenta con un conjunto de redes de empresas, muchas de la cuales tienen hoy el reto de seguir siendo exitosas, mediante una formidable transformación de su visión del entorno y la orientación de sus habilidades y potencialidades. Hoy por hoy el éxito de una empresa no depende solamente del producto que ofrece como en los años 70's y 80's. También necesita involucrar los servicios que le presta al cliente y la forma como desarrolla sus procesos administrativos para garantizar su permanencia en el mercado y por ende su triunfo. De esta manera, han entendido que un elemento crítico para su éxito y supervivencia, es la administración efectiva de la información y de la Tecnología de Información (IT) relacionada.

Es aquí donde SEVICOL LTDA., se identifica notablemente y quiere pasar de ser una empresa que reconoce los beneficios potenciales que la tecnología puede proporcionar, a una empresa EXITOSA que también comprende y administra los riesgos asociados con la implementación de nueva tecnología.

Por esto, y para poder afrontar el problema planteado en este documento se propone ejecutar una Auditoría Informática que realice un estudio de riesgos y diseñe controles según los estándares fiduciarios y de seguridad del modelo COBIT 3ra. Edición, y que además, contribuya a la implantación del sistema de control interno

informático de la compañía con el fin de garantizar la perennidad y el alcance de objetivos planteados en la organización.

1.3.1 DESCRIPCIÓN DE LOS ALCANCES DEL PROYECTO

- Al elaborar un documento que contenga la configuración del entorno informático de SEVICOL LTDA., podremos identificar posibles riesgos y definir los controles a implementar en varios niveles diferentes según el grado de competencia de cada usuario.

- A partir de la siguiente definición de Control Interno:

  Conjunto de medidas que contribuyen al dominio de la empresa. Tiene como finalidad, por un lado, asegurar la protección y salvaguarda del patrimonio y la calidad de la información, y por otro, la aplicación de las instrucciones de la dirección y favorecer la mejora de las actuaciones. Se manifiesta por medio de la organización, los métodos y procedimientos de algunas de las actividades de la empresa para mantener la perennidad de la misma[4].

  Se hace mas claro lo que lograremos en nuestro segundo objetivo que es el de Implantación del Sistema de Control Interno Informático lo que garantizara la operatividad del entorno informático de la empresa.

- El estudio de los riesgos informáticos nos permitirá medir el grado de exposición al que se encuentra cada segmento del entorno informático de la compañía y así establecer prioridades de implementación de controles.

- Definición de Controles, con el cumplimiento de este objetivo se conseguirá que la empresa cuenta con procedimientos y practicas que garanticen razonablemente que los objetivos del negocio sean alcanzados y que eventos no deseados sean prevenidos o detectados y corregidos.

Como efecto de todo este proceso de Auditoría, SEVICOL LTDA., seguirá siendo la empresa líder, la que ha acostumbrado a sus clientes a ofrecer los mejores servicios ya que no ahorra esfuerzo y no escatima detalle en la consecución de procesos administrativos que le garantizan ser la número uno en la región en la prestación de servicios de seguridad y vigilancia privada.

[4] YANN, Derrien. Técnicas de la auditoría informática, Ediciones Alfaomega S.A., México 1995 p. 7

2. MARCO TEORICO

2.1 LA AUDITORIA INFORMATICA: DEFINICIÓN

Tabla 2.1 Algunas definiciones de Auditoría Informática

Referencia Bibliográfica	Definición de Auditoría Informática
http://dmi.uib.es/~bbuades/auditoria/ **Autor:** CAIB	Es el conjunto de técnicas, actividades, y procedimientos, destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control de eficacia, seguridad y adecuación del servicio informático en la empresa, por lo que comprende un examen metódico, puntual y discontinuo del servicio informático, con vistas a mejorar en: Rentabilidad, Eficiencia y ayudar a asegurar la confiabilidad de los Estados Financieros y el cumplimiento de las Leyes y Regulaciones.
Derrien, Yann. Técnicas de la auditoría informática. (1994, p. 2-3)	La Auditoría Informática se trata de un conjunto de técnicas muy diversas que permiten dar respuesta a objetivos también muy variados. Para el Director General, poco versado en la materia, se trata de "ver un poco más clara" la actividad de unos de los servicios clave de su empresa. Para el Director Informático, aporta, además de un asesoramiento sobre la organización, dado por especialistas externos, el medio de seguir y justificar la aplicación de nuevas estructuras o de nuevos métodos. El Director Financiero, en lo que le concierne, verá más a menudo el medio de estimar la fiabilidad de las cadenas del proceso, de las cuales él es el usuario.
Valriberas, Sanchez Gloria. AUDITORÍA INFORMÁTICA Un enfoque práctico. (2001, p.28-29)	Es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos
Hernández (1996, p-18)	Un proceso formal ejecutado por especialistas de auditoría y de informática; se orienta a la verificación y aseguramiento de que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología informática en la organización se lleven a cabo de una manera oportuna y eficiente

2.2 El estándar COBIT: Misión y Conceptos

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

COBIT® (Control Objetives By Information Technology) nace para dar respuesta a la necesidad de los empresarios de administrar las Tecnologías de la Información que apoyan los procesos administrativos y operativos en la Organización. Reconociendo además, el gran impacto que tienen los recursos tecnológicos y humanos en el éxito de la empresa y las grandes inversiones que se hacen en el área tecnológica, contrastada a veces con el poco aporte que se recibe de esta.

Por lo tanto, la administración de la misma forma que controla su área financiera y productiva estableciendo controles adecuados, debe entender que se hace necesario y prioritario hacer lo mismo con su área tecnológica, estableciendo mecanismos que le permitan tener una apreciación y un entendimiento básico de los riesgos y limitantes del empleo de tecnologías de la información.

Para poder cubrir esta nueva necesidad y alcanzar las expectativas que se esperan de la función informática se hace necesario definir un sistema adecuado de CONTROL

INTERNO INFORMATICO que garantice en la medida de lo posible la correcta y eficiente forma de administrar el recurso tecnológico.

Teniendo bien definido lo que se deseaba alcanzar, ISACF Information Systems Audit and Control Foundation y un grupo de investigadores y catedráticos estadounidenses y europeos desarrollaron un estándar de administración de Tecnologías de Información denominado COBIT, el cual reconoce que un elemento critico para el éxito y supervivencia de las organizaciones es la efectiva administración de la información y las Tecnologías de la información relacionadas.

A continuación, hacemos una breve descripción de cómo se presenta el modelo COBIT. Comienza con la siguiente premisa.

> *Con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos, los recursos de TI (Tecnologías de la Información) deben ser administrados por un conjunto de procesos de TI agrupados en forma natural. COBIT® OBJETIVOS DE CONTROL, ISACF (1998, p6)*

Continua con un conjunto de 34 Objetivos de Control[5] de alto nivel, uno para cada uno de los Procesos de TI, agrupados en cuatro Dominios: Planeación & Organización, Adquisición & Implementación, Entrega (de servicios) y

[5] Una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control en una actividad de TI particular. ISACF (1998, p12)

Monitoréo. Esta estructura cubre todos los aspectos de información y de la tecnología que la soporta.

Análogamente, COBIT otorga especial atención al impacto sobre los Recursos de TI, así como a los requerimientos de negocios en cuanto a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

Tabla 2.2 Requerimientos de la Información definidos en el modelo COBIT

Requerimientos de la Información	**Definición**
Efectividad	Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
Eficiencia	Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.
Confidencialidad	Se refiere a la protección de información sensible contra divulgación no autorizada.
Integridad	Se refiere a la precisión y suficiencia de la información. Así como a su validez de acuerdo con los valores y expectativas del negocio.
Disponibilidad	Disponibilidad de la información cuando esta es requerida por algún proceso del negocio. También, se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
Cumplimiento	Cumplimiento de leyes, regulaciones y acuerdos contractuales a los que el proceso de negocio este sujeto.
Confiabilidad de la Información	Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

Tabla 2.3 Recursos de TI identificados por el modelo COBIT

Recursos de TI	Definición
Datos	Los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.
Aplicaciones	Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados
Tecnología	La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.
Instalaciones	Recursos para alojar y dar soporte a los sistemas de información.
Personal	Habilidades del personal, conocimiento, conciencia, y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

Tabla 2.4 Definición de los dominios según el modelo COBIT

DOMINIO	DEFINICIÓN
Planeación y Organización	Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una estructura tecnológica apropiadas.
Adquisición e Implementación	Para llevar a cabo la estrategia de TI, las soluciones de TI deber ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

Entrega y Soporte	En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesario.
Monitoréo	Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

Finalizando podemos notar que COBIT® se presenta como una herramienta para administrar TI ayudando al entendimiento y la administración de los riesgos y definiendo los controles asociados con el uso de Tecnologías de la Información.

2.3 Tres modos sobre las funciones del Auditor Informático

La auditoría informática ha evolucionado en los métodos y técnicas utilizadas para cumplir con su objetivo que es el de: emitir una opinión profesional sobre la eficacia y eficiencia del funcionamiento del entorno informático en una organización. Lamentablemente en sus comienzos la AI solo se conformaba con emitir reportes acerca de las anomalías encontradas y tan solo se presentaba como complemento a la Auditoría Financiera y en poco contribuía en aportar soluciones al entorno informático, de ahí, tal vez la poca importancia que se le daba a este tipo de trabajo. Sin embargo, debido al gran impacto que tienen las tecnologías de la información para ayudar a alcanzar los objetivos en la empresa, los empresarios no dudan ahora en invertir en recurso técnicos, tecnológicos y humanos en pro de la consecución del éxito empresarial lo que ha conllevado a la necesidad de administrar eficientemente la función informática.

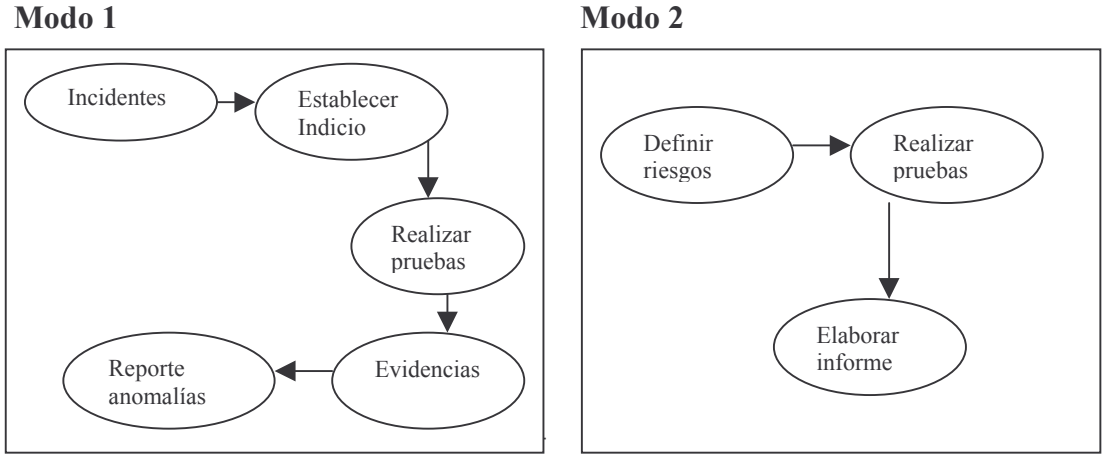
A continuación se presentan tres modos acerca de las funciones del Auditor Informático donde se puede notar la evolución en el carácter protagónico de este servicio en el apoyo a las funciones y objetivos del entorno informático en la empresa.

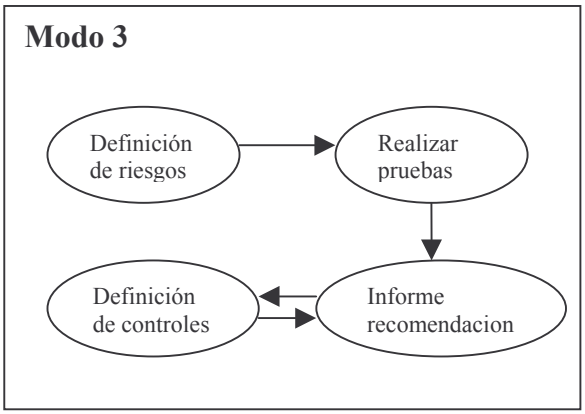
Tabla 2.5 Breve descripción de cada uno de los Modos de las funciones de la AI

MODOS	DESCRIPCION
Modo 1	A partir de unos incidentes, indagamos y establecemos indicios que pudieron haber originado el incidente, realizamos pruebas de comprobación y registramos evidencias para por ultimo entregar el respectivo informe.
Modo 2	En este modo definimos los tipos de riesgos a estudiar, realizamos las pruebas necesarias para asegurarnos del cumplimiento o no de la actividad y elaboramos el respectivo informe.
Modo 3	Al igual que el anterior, definimos los tipos de riesgos, realizamos pruebas para asegurarnos del cumplimiento o no del objetivo de la actividad y elaboramos un primer informe del trabajo hasta ahora, luego definimos los controles respectivos para asegurarnos del cumplimiento del objetivo de la actividad y entregamos un ultimo informe.

A diferencia de los dos modos iniciales donde el auditor solo se limita a opinar sobre el estado actual del entorno informático el modo tres se presenta como ayuda al auditado ya que propone controles y recomendaciones para asegurar el cumplimiento de los objetivos de este departamento.

Figura 2.1 Modos de las funciones del Auditor Informático





2.4 Marco Jurídico de la Auditoría Informática

La repercusión que las nuevas tecnologías de la información han generado en las organizaciones empresariales es tal que las TI se han convertido en un activo más y muy preciado para las empresas lo que ha originado en pensar y diseñar mecanismos para su salvaguarda y protección.

De la misma forma que las nuevas tecnologías de la información han transformado el modo de operar de los diferentes sectores empresariales tanto públicos como privados, profesionales y particulares esta incidencia también ha recaído en el Derecho desde dos perspectivas:

1. Contemplar estas nuevas tecnologías como una herramienta del operador jurídico de forma parecida a como ayudan a otros profesionales: arquitectos, médicos, etc. Lo que da lugar a la Informática Jurídica.

2. Estudiar y analizar estas nuevas tecnologías como un objeto del Derecho, lo que hace emerger una rama nueva del mismo: el Derecho Informático[6]

El Derecho Informático es la rama del derecho que regula el ambiente informático, controlándolo y no permitiendo que se convierta en una torre de Babel. Como resultado de este nuevo enfoque del derecho, podemos considerar: la protección de datos personales, la protección jurídica del software, los delitos informáticos, el documento electrónico, el comercio electrónico y la contratación electrónica e informática entre otras.

El auditor informático si quiere ejercer bien su labor y evitar sorpresas desagradables debe conocer esta nueva rama jurídica que regula su actividad, "el que inocentemente peca, inocentemente se condena".

A continuación hacemos una breve descripción de los principios que regulan la protección de datos (Ley Orgánica 15/1999, España).

[6] Mario Gerardo Piattini Velthuis, Emilio del Peso Navarro. Auditoría Informática Un enfoque práctico. Madrid, 1998. p119

Tabla 2.6 Descripción de principios de protección de datos

Principio	**Descripción**
Finalidad	Antes de la creación de un archivo de datos de carácter personal, ha de conocerse el fin del mismo.
Pertinencia	Los datos deben ser pertinentes, es decir estar relacionados con el fin perseguido al crearse el archivo.
Utilización Abusiva	Los datos recogidos no deben ser utilizados para otro fin distinto a aquel para el que fueron recabados.
Exactitud	El responsable de los archivos debe asegurarse de la exactitud de los datos recogidos y su puesta al día.
Derecho al olvido	Los datos deberán ser eliminados de los archivos una vez cumplido su fin.
Consentimiento	El tratamiento automatizado de los datos requerirá del consentimiento del afectado salvo disposiciones de ley.
Protección especial de datos	Se debe garantizar de forma especial el tratamiento de los datos de carácter personal cuando ellos se refieran a ideologías, religión, vida sexual, salud, etc.
Seguridad	El responsable deberá adoptar las medidas necesarias de índole física, organizativa o lógica con objeto de poder garantizar la seguridad de los datos de los archivos.
Acceso individual	Cualquier persona tendrá derecho a saber si sus datos son tratados de forma automatizada y tener copia de los mismos. De igual forma tiene derecho de que estos sean exactos y corregidos o destruidos.
Publicidad	Es necesario que exista un archivo público en el que figuren los diseños de los archivos de datos de carácter personal, tanto los de titularidad pública como privada.

2.4.1 Delitos Informáticos

Delito es el quebrantamiento de la ley luego por analogía podemos decir que delito informático es el quebrantamiento de las leyes que regulan la informática y lo referente con las nuevas tecnologías de la información.

Los elementos integrantes del delito son:

- El delito es un acto humano, es una acción (acción y omisión)
- Ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.
- Debe corresponder a un tipo legal (figura de delito), definido por la ley, ha de ser un acto típico.
- El acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia).
- La ejecución u omisión del acto debe estar sancionada con una pena.

Ahora, viendo el delito informático en su más amplio sentido se pueden definir algunas figuras delictivas.

Tabla 2.7 Algunas figuras delictivas.

Figuras Delictiva	Delito
Contra la intimidad	Estafa Informática
Contra el Patrimonio	Defraudación
Falsedad Documental	Daño Informático
	Propiedad Intelectual

2.5 Riesgo, Control y Prueba

Como herramienta que tiene el Auditor Informático, para el éxito d su trabajo.[7]

2.5.1 Definición de Riesgo

El concepto de riesgo puede definirse como la probabilidad que un evento no deseado pueda ocurrir.

2.5.1.1 Tipos de Riesgos

1. **Riesgo Inherente**

   Se entiende como aquel conjunto de situaciones peligrosas, derivadas de la naturaleza propia de un fenómeno o sistema y sobre

[7] La definición, clasificación, y aplicación de los conceptos de Riesgo, Control y Prueba fueron tomadas del Curso de Auditoría de Sistemas del Ing. Luis Carlos Gómez Florez, de la UIS.

las cuales se habrán de desarrollar estudios de riesgos. Para establecer las posibles acciones de control.

2. **Riesgo de Control**

   Dada una situación de riesgo inherente, si para ella se definen un conjunto de mecanismos de control, aquella posibilidad de que estos controles no sean suficientes o deficientes, se denomina riesgo de control.

2.5.2 Definición de Control y su clasificación

Control se define como: Las políticas, procedimientos, practicas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos. ISACF, COBIT (1998, p 12)

Los controles se pueden clasificar de cuatro formas:

- De acuerdo a la forma como ha de actuar
- Según su línea de acción
- Según su naturaleza
- Según su acción

2.5.2.1 Controles Directos y Generales

De acuerdo a la forma como ha de actuar un control, éstos se pueden dividir en controles directos y controles generales.

- **Controles Directos**

  Son aquellos que actúan de manera directa sobre el espacio de riesgo, es decir mediante acciones que van dirigidas hacia los elementos causales del posible riesgo.

- **Controles Generales**

  De forma complementaria a los controles directos, existen otros controles que no actúan de manera particular sobre un determinado riesgo, sino que actúan de manera global sobre la multitud de riesgos, los cuales se denominan controles generales

2.5.2.2 Controles Horizontales y Verticales

Según su línea de acción, los controles se pueden dividir en controles horizontales y controles verticales o jerárquicos.

- **Controles Horizontales**

  Se pueden realizar en cualquier orden y por tanto no altera en nada el control.

- **Controles Verticales o Jerárquicos**

  Son controles que tienen que seguir una línea de acción. Se establecen para pasar de una lugar a otro. Ej: la firma que autoriza que un documento puede pasar al computador.

2.5.2.3 Controles Lógicos y Técnicos

Según su naturaleza, los controles se dividen en lógicos y técnicos.

- **Controles Lógicos**

  Son aquellos que cambian la acción lógica de las cosas (alternan la secuencia). Ej: verificar si se pude o no hacer un retiro.

- **Controles Técnicos.**

  No cambian l acción lógica de las cosas. Ej: Codígito (dígito para verificar errores).

2.5.2.4 Controles Preventivos, Detectivos y Correctivos

De acuerdo al rol que ocupa un control con respecto al riesgo correspondiente, es decir, si contribuye a descartar una situación de riesgo, a detectar los errores, éstos se pueden dividir en controles preventivos, detectivos y correctivos.

- **Controles Preventivos**

  Son los más económicos. Se realizan antes de que suceda la acción y reducen la frecuencia con que ocurren las causas del riesgo, generalmente son del tipo de advertencias (ej: Prohibido el paso, No fumar).

- **Controles Detectivos**

  Son aquellos que detectan el error cuando el proceso esta en curso.

- **Controles Correctivos**

  Son los más costosos, tienden a superar los problemas una vez hayan sucedido.

2.5.3 Riesgos y Controles en Sistemas Informáticos

En la siguiente tabla se presentan los siete niveles de riesgo y controles identificados según Price Waterhouse en Sistemas Informáticos

Tabla 2.8 Niveles de riesgo y sus controles en Sistemas Informáticos

Riesgo	Definición	Medios de Control
Acceso a funciones de procesamiento	Consiste en que personas no autorizadas puedan acceder a funciones del software de aplicación, permitiéndoles leer, modificar, agregar, eliminar datos o registros, o procesar transacciones no autorizadas	La segregación de funciones y e control de acceso
Ingreso de Datos	Consiste en que los datos que ingresan para ser procesados o almacenados puedan ser imprecisos, incompletos o ingresados más de una vez	Controles de edición y validación, controles de lote y doble digitación de campos críticos.
Items rechazados o en suspenso	Surgen cuando las transacciones rechazadas y pendientes pueden no ser detectadas, analizadas y corregidas	Controles programados y controles de usuario.
Procesamiento	Consiste en que las transacciones procesadas o generadas por el sistema pueden perderse o ser procesadas o registradas en forma incompleta, inexacta o en el periodo contable incorrecto.	Formularios prenumerados, rutinas de control de secuencia, controles de balanceo, de lote, rótulos de archivos, transmisión de datos y procedimiento de enganche y recuperación.
Estructura organizativa del Dpto. de sistemas	Surge cuando la estructura organizacional y/o los procedimientos operativos del Departamento de sistemas no garantizan un ambiente de procesamiento que conduzca al manejo adecuado de la información.	Segregación de funciones en el Dpto. de sistemas y controles y procedimientos operativos.
Cambios a los programas	Consiste en que los programadores pueden efectuar cambios incorrectos y/o no autorizados en el software de aplicación.	Procedimientos de iniciación, aprobación y documentación, procedimientos de catalogación y mantenimiento, intervención de los usuarios, procedimientos de prueba y supervisión efectiva.
Acceso general	Surge cuando personas no autorizadas pueden tener acceso a los archivos de datos o a los programas permitiéndoles leer, modificar, agregar o eliminar algún ítem o segmento de programas.	Software de control de acceso, análisis de Logs e informes gerenciales, control de acceso físico y protección de datos.

2.5.4 Pruebas Sustantivas y de Cumplimiento

2.5.4.1 Definición de Prueba

Análogamente a la definición de riesgos como la posibilidad de falla o daño y control como los mecanismos necesarios para disminuir o evitar riesgos, podemos decir que prueba es aquel procedimiento que permite comprobar el adecuado funcionamiento de un proceso de control o establecer evidencia de validez de una operación o actividad.

2.5.4.2 Pruebas de cumplimiento

Las pruebas de cumplimiento se usan para comprobar que se están cumpliendo las normas y reglas establecidas. Es decir, para comprobar la eficacia y eficiencia de los mecanismos de control establecidos. Dentro de los procedimientos que se pueden utilizar como pruebas de cumplimiento se destacan:

Tabla 2.9 Procedimientos para la realización de las pruebas de cumplimiento

Procedimiento	Definición
Indagaciones y manifestaciones	Por su carácter de testificación, se denominan pruebas testimoniales. Cuando el auditor toma la iniciativa son llamadas indagaciones y cuando el personal ajeno al equipo auditor toma la iniciativa se denominan manifestaciones.
Observaciones	Son útiles cuando el tiempo que se tiene para realizarlas es lo suficientemente prolongado para obtener conclusiones.
Procedimientos de diagnóstico	El diagnóstico se basa en el análisis de una serie de indicadores de estado del sistema y la correlación que estos presentan, frente a la conducta ideal del sistema.
Inspección de documentación del sistema	Se basa en la recolección de pruebas documentales que en algunos casos permiten corroborar fallas o fraudes por su existencia falsificada, inexistencia o en otros casos por su pérdida.
Técnica de datos de prueba	Se pretende mediante estos procedimientos, seleccionar un conjunto de datos que contengan información tan precisa o imprecisa que permita establecer que controles no están actuando convenientemente.

2.5.4.3 Pruebas Sustantivas

Las pruebas sustantivas son la que se efectúan en aquellos casos en los cuales no existen controles adecuados y permiten a través de su ejecución obtener

evidencias suficientes. Dentro de los procedimientos catalogados como pruebas sustantivas se encuentran además de indagaciones y manifestaciones las siguientes:

- Procedimientos analíticos: Estos procedimientos son utilizados cuando existe gran dificultad de aplicar otros o cuando se desea obtener unos márgenes más altos. Estos son, verificaciones de razonabilidad y análisis de tendencias históricas aquí se analiza el comportamiento de una variable frente al comportamiento esperado y razonable; cálculo y análisis de índices consisten en la relación matemática de dos o más variables por medio de la relación razonable entre ellas.

- Pruebas detalladas de transacciones y saldos: estas pruebas se ejecutan cuando es necesario corroborar con total certeza la validez de una transacción o la veracidad de un saldo lo cual se puede hacer a través de: Inspección de documentos y registros soportes, inspección física de los objetos (inventarios), confirmación externa con el sujeto generador de la transacción y reproducción o reejecución de la transacción con el fin de comprobar en detalle la acción de los controles.

2.5.5 Control Interno Informático: Definición

Según el informe del Committee of Sponsoring Organization of the Treadway Commission (COSO) control interno se define así:

Control interno en un proceso, ejecutado por el consejo de directores, la administración y otro personal de una entidad, diseñado para proporcionar seguridad razonable con miras a la consecución de objetivos en las siguientes categorías:

- Efectividad y eficiencia de las operaciones
- Confiabilidad en la información financiera
- Cumplimiento de las leyes y regulaciones aplicables

De esta definición se desprenden algunos conceptos fundamentales:

- El control interno es un proceso. Constituye un medio para un fin, no un fin en si mismo.
- El control interno es ejecutado por personas. No son solamente manuales de políticas y formas, sino personas en cada nivel de una organización.
- Del control interno puede esperarse que proporcione solamente seguridad razonable, no seguridad absoluta, a la administración y al consejo de una entidad.
- El control interno está engranado para la consecución de objetivos en una o más categorías separadas pero interrelacionadas

Siguiendo con la idea que esta definición nos ofrece, por analogía podemos decir que el control interno informático es el conjunto de medidas que nos permiten dominar en la medida de lo posible el área informática. Tiene como finalidad, asegurar la protección, salvaguarda y calidad en cuanto a recursos técnicos, tecnológicos y de información que competen en este entorno tecnológico. Se manifiesta por medio de la organización, los métodos y procedimientos de esta área en la empresa para mantener la perennidad de la misma.

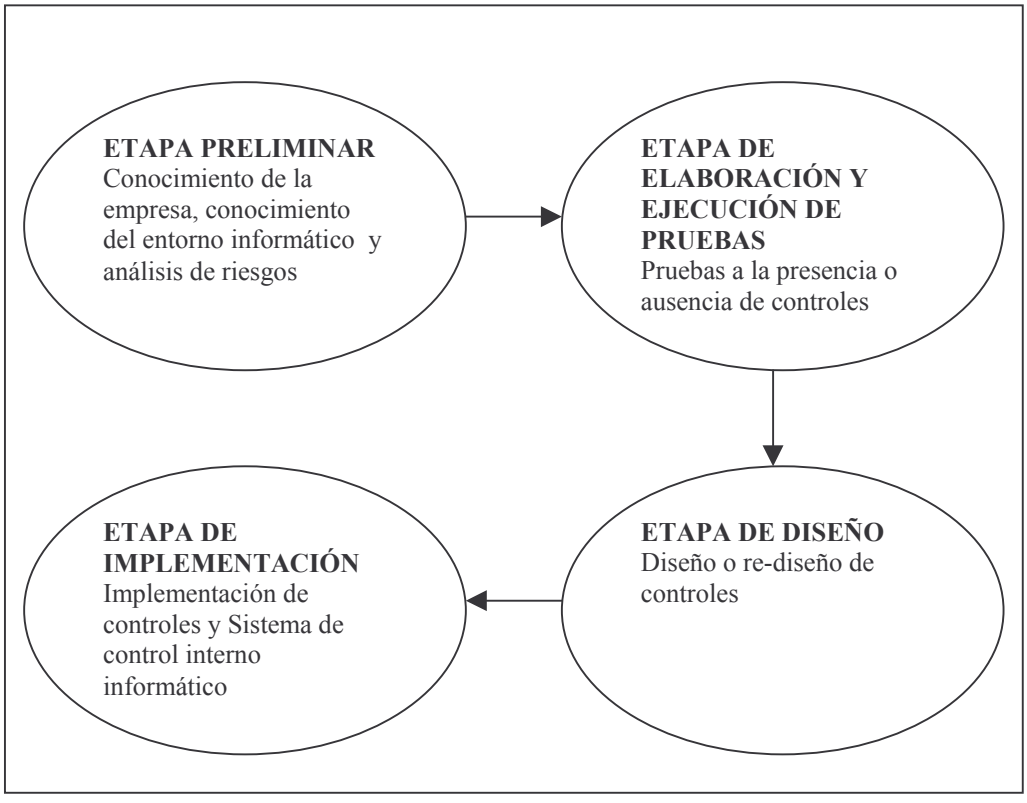
A continuación, se presenta los principios básicos de organización que satisface la actividad informática. Es decir, una lista de áreas que hacen parte del marco aceptado de control interno informático.

- La organización general del entorno informático.
- Los procedimientos de desarrollo y mantenimiento del software.
- El entorno de producción.
- Funciones técnicas.
- Protección y confidencialidad de datos.

3. METODOLOGÌA PARA LA AUDITORIA INFORMATICA

Reconociendo la importancia que representa para el éxito de este trabajo la correcta elección de una metodología que guíe paso a paso la ejecución de la Auditoría conviene mencionar que haremos una adaptación a nuestro caso de la Metodología de Auditoría propuesta por Nicolas Leuro y William Tristancho en su tesis de grado (Auditoria del Sistema de Información Académica de la Corporación Educativa ASED, UIS 2003). Esta metodología comprende cuatro etapas como se muestra en la siguiente figura.

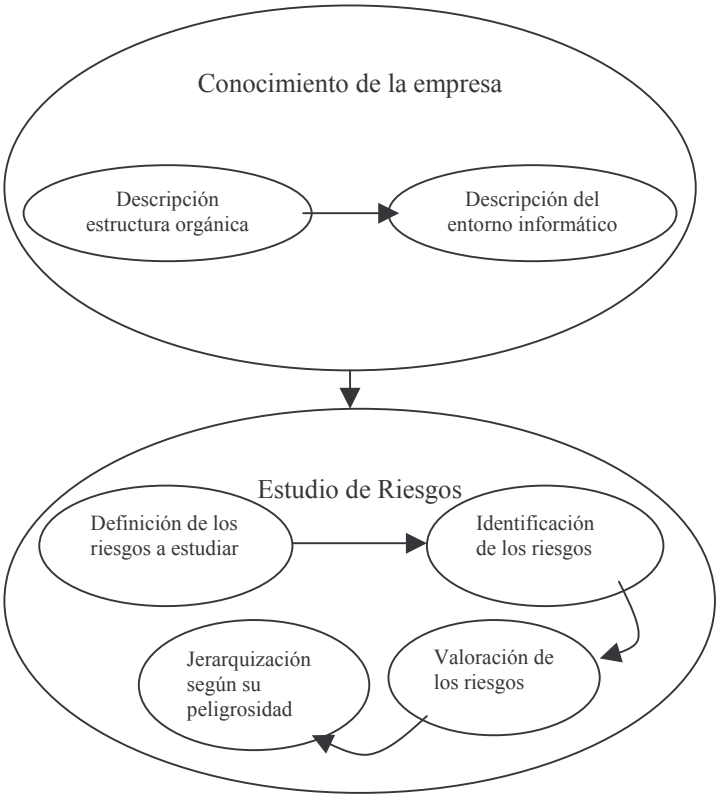
Figura 3.1 Las cuatro etapas de la metodología para la auditoría de sistemas



3.1 ETAPA PRELIMINAR

La Auditoria Informática exige un profundo conocimiento del entorno a auditar, por lo que se hace necesario hacer un estudio detallado en lo que corresponde al contexto organizacional y los riesgos asociados con el uso de tecnologías de la información que apoyan los procesos administrativos en la empresa.

Figura 3.2 Componentes y pasos de la etapa preliminar



3.1.1 CONOCIMIENTO DE LA EMPRESA

El conocimiento de la empresa, tal como se muestra en la figura 3.1, comprende: Descripción de la estructura orgánica, descripción del entorno informático y descripción de los procesos y actividades.

3.1.1.1 Descripción de la estructura orgánica

La descripción de la estructura orgánica de la empresa donde ocurre la situación problema, se realiza mediante la inspección de su documentación, la realización de entrevistas con su directivos y el contacto directo con las diferentes personas de interés, tratándose con ello de identificar sus órganos, de conocer sus misiones e interacciones, así como su papel en la formulación de políticas, procedimientos, normas y controles, a fin de facilitar el accionar de los auditores.

Es aquí, en este paso a partir de la opinión de la alta dirección, que determinamos el grado de confianza y satisfacción que tiene en los productos, servicios y recursos de informática del negocio, además detectamos fortalezas, aciertos y apoyo que brinda el área en estudio desde la perspectiva de las directivas de la empresa y los usuarios en general y por último, determinamos cuales son las áreas de oportunidad que tiene el entorno informático para hacer más rentable y competitivo el negocio.

3.1.1.2 Descripción del entorno informático

Luego de conocer la estructura organizacional, el siguiente paso de la auditoría informática es familiarizarse con el entorno informático, identificando sus sistemas componentes, recursos e interacciones es decir, lo que corresponde al documento de configuración del sistema informático en la empresa que se describe en el primer objetivo especifico de este informe.

3.1.2 EL ESTUDIO DE RIESGOS

Luego de haber logrado el conocimiento de la empresa y del entorno informático a auditar, queda abierto el campo de acción para el estudio de riesgos, para lo cual es necesario definir el tipo de riesgos a estudiar para posteriormente adelantar el proceso de identificación, valoración y jerarquización de acuerdo a el grado de peligrosidad.

3.1.2.1 Definición de los riesgos a estudiar

La definición de los riesgos a tener en cuenta en nuestro trabajo de auditoría informática, nos da la posibilidad de limitar los alcances de la misma y los compromisos que vamos a asumir “Definid y no discutiréis”, es decir, para nuestro caso los asociados con el uso de tecnologías de la información que apoyan los procesos operativos y administrativos y los principios básicos de

organización dentro de un marco aceptado de Control Interno Informático como se menciono en el capitulo 2.

3.1.2.2 Identificación de los riesgos

Luego de haber definido el tipo de riesgos a estudiar, a partir de la información obtenida en el conocimiento de la empresa, se estudia sistemáticamente los procesos y las tecnologías incorporadas para identificar los riesgos presentes.

3.1.2.3 Valoración de los riesgos

Una vez identificados los riesgos del entorno informático auditado, es necesario valorar su impacto y establecer su grado de peligrosidad, lo cual presupone un registro estadístico y sistemático de los incidentes y accidentes relacionado con la información, sin embargo, como muchas empresas no lo hacen, es necesario para cada caso diseñar un sistema de valoración ajustado a la características y disponibilidades de información. Las metodologías de estudios de riesgos aplicadas en salud ocupacional son una buena guía a ser utilizadas. De igual forma, la experiencia del personal vinculado en la empresa y de auditoría ayudará a contrarrestar el efecto de la ausencia de información estadística.

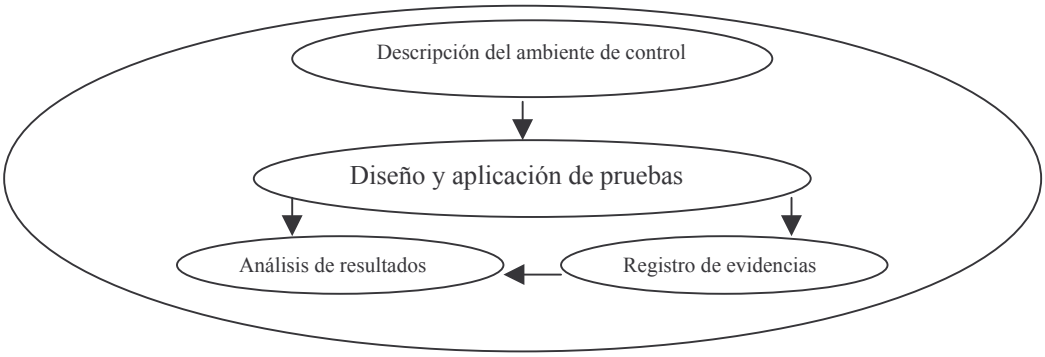
3.1.2.4 Jerarquización de riesgos según su grado de peligrosidad

La valoración de los riesgos en términos de su grado de peligrosidad, permitirá jerarquizarlos para establecer un orden de prioridad que oriente las acciones predictivas, preventivas y correctivas derivadas de la acción de auditoría, así como los horizontes de tiempo (Inmediato, corto, mediano y largo plazo) en que habrán de llevarse cabo.

3.2 ETAPA DE ELABORACIÓN Y EJECUCIÓN DE PRUEBAS

El estudio de riesgos da paso a la etapa de elaboración y ejecución de pruebas que permiten evaluar los controles existentes y detectar los que hacen falta. Para los primeros se aplican pruebas de cumplimiento y para los segundos las pruebas sustantivas.

Figura 3.3 Pasos de la etapa de ejecución y elaboración de pruebas



3.2.1 Descripción del ambiente de control

La elaboración y ejecución de pruebas requiere de la descripción del ambiente de control como prerrequisito para la localización de puntos de control.

Aquí reconocemos que el elemento esencial del ambiente de control de una empresa es su gente, sus atributos individuales, incluyendo la integridad, los valores éticos y la competencia y el ambiente en que ella opera.

3.2.2 Diseño y localización de pruebas

Una vez identificados los controles existentes y las ausencias de estos, se procede al diseño de las respectivas pruebas de cumplimiento y sustantivas cuya aplicación se hará seleccionando los tipos y procedimientos apropiados,

descritos en el capitulo 2, finalmente se organizan y se procede a su aplicación y registro de resultados.

3.2.3 Registro de evidencias

La aplicación de pruebas puede conducir al descubrimiento de evidencias de eventos indeseables (manifestaciones de riesgo) las cuales, siempre que sea posible deben registrarse o documentarse, pues constituyen una eficiente forma de respaldo de los resultados obtenidos.

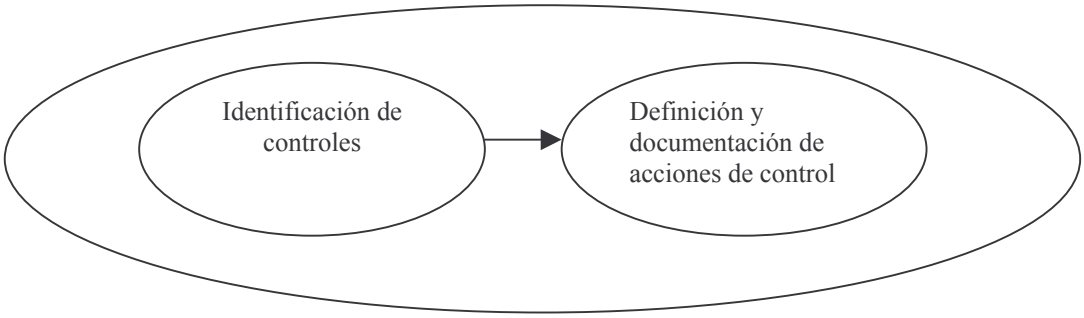
3.2.5 Análisis de resultados

Este procedimiento nos permite comprobar que tan expuesto esta el proceso por los riesgos identificados lo que nos permite garantizar la orientación y validez que tendrá el control sobre los riesgos pertinentes y definir la prioridad de su implementación.

3.3 ETAPA DE DISEÑO DE CONTROLES

El análisis de los resultados de las pruebas conduce al diseño de los controles que sea necesario mejorar o construir, los cuales, como se expuso en el capitulo 2, se clasifican según su cobertura y finalidad en detectivos, preventivos y correctivos o en directos y generales.

Figura 3.4 Pasos de la etapa de diseño



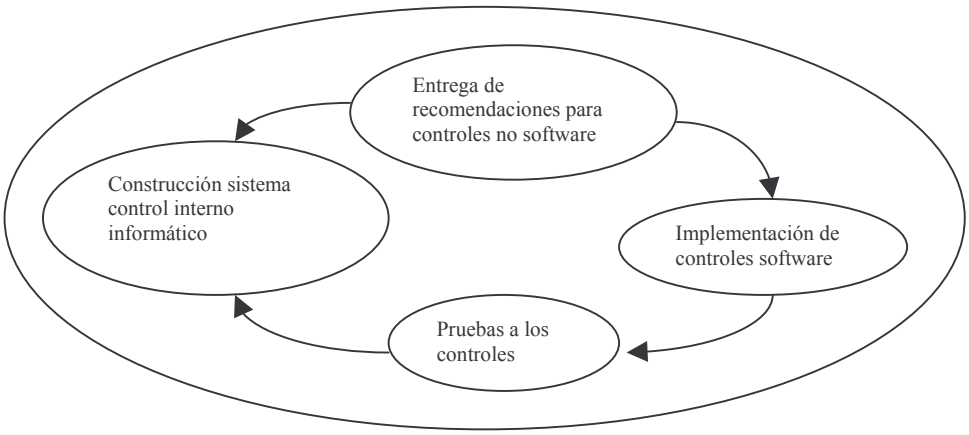
El diseño de controles se realiza en dos pasos como se muestra en la anterior figura, comenzando con su identificación, necesaria para distinguirlos unos de otros, la cual se enfoca desde dos puntos de vista: el primero identifica los controles que no se pueden implementar haciendo uso de software, tal como la creación de un nuevo formato para el registro manual de información; el segundo, identifica los controles software susceptibles de implementarse y que se pueden incorporar en las aplicaciones que procesan datos.

El segundo paso del diseño de controles, es la definición y documentación de cada una de sus acciones.

3.4 ETAPA DE IMPLEMENTACIÓN

Una vez se han diseñado los controles, se da paso a la última etapa de la metodología, que como su nombre lo indica, es aquella donde se implementan los controles diseñados al igual que el sistema de control interno informático.

Figura 3.5 Pasos de la etapa de implementación



La metodología para el desarrollo de la Auditoría informática consta de cuatro etapas: preliminar, ejecución y elaboración de pruebas, diseño de controles e implementación. En la siguiente tabla se resume los paso que componen cada etapa.

Tabla 3.1 Resumen metodología para la Auditoría Informática

ETAPA	PASO	DESCRIPCION
Preliminar: conocimiento de la empresa	Descripción estructura orgánica	Revisión de la documentación y entrevistas con alta dirección y personal de interés para la auditoría
	Descripción del Entorno informático	A partir de la entrega de la configuración del sistema informática de la empresa.
	Descripción de los procesos y actividades del entorno informático	Selección de procesos administrativos vitales y diseño de flujos de datos.
Preliminar: Estudio de Riesgos	Definición de los riesgos a estudiar	En el caso de la Auditoría Informática los relacionados con el uso de las tecnologías de la información.
	Identificación de los riesgos	A partir del conocimiento de la empresa y en los procesos y tecnologías presentes.
	Valoración de los riesgos	Construcción de un modelo de valoración en términos de grado de peligrosidad, según su probabilidad de impacto.
	Jerarquización de los riesgos	A partir del resultado del modelo de valoración.
Elaboración y ejecución de pruebas	Diseño y aplicación de pruebas	Se utilizan las pruebas descritas en el capitulo 2.
	Análisis de resultados y hallazgo de evidencias	Análisis de los resultados de las pruebas, obtención de evidencias a partir de las pruebas efectuadas.
Diseño de controles	Identificación de controles	De las conclusiones del análisis de pruebas
	Definición y documentación de acciones de control	Se definen las acciones de control a realizar con su respectiva documentación
Implementación	Entrega de recomendaciones	Reunión con los encargados de la función informática para definir si es posible su implementación
	Implementación de controles software	Utilizando la herramienta de desarrollo que posee la empresa

	Construcción del sistema de control interno informático	Definición de políticas, procedimientos y acciones para administrar el entorno informático

4. APLICACIÓN DE LA METODOLOGÍA EN SEVICOL

4.1 ETAPA PRELIMINAR

En esta etapa se presenta los resultados de las actividades realizadas durante la ejecución de la primera fase de la metodología de auditoría informática propuesta en el capitulo anterior.

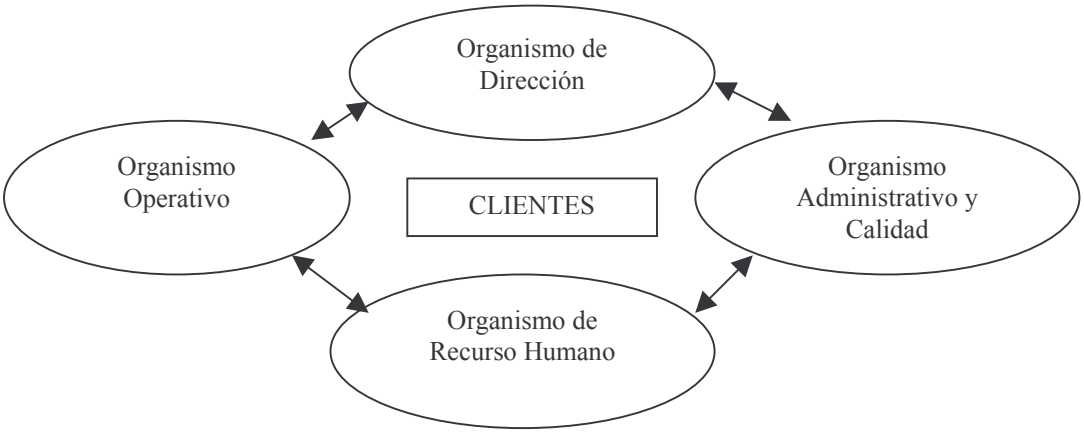
4.1.1 CONOCIMIENTO DE LA EMPRESA: ACERCA DE SEVICOL LTDA.

En este apartado el lector podrá remitirse a la primera parte, presentación del proyecto, de este informe donde se relata desde el inicio de la empresa, los servicios que presta y su evolución tecnológica.

4.1.2 Descripción de la estructura orgánica

SEVICOL LTDA, presenta un modelo organizacional orientada al cliente debido a su objeto comercial como prestadora de servicios de seguridad y vigilancia. Para cumplir con sus objetivos se han estructurado cuatro organismos responsables de llevar a feliz término su misión empresarial.

Figura 4.1 Organigrama General de Sevicol Ltda.



El organismo directivo tiene como objetivos representar legalmente la empresa, definir metas, el crecimiento corporativo, presupuestos inversiones y salarios. Además, velar por el cumplimiento de las metas administrativas y financieras como también, hacer crecer la compañía basado en análisis de mercado y del área financiera.

Organismo Administrativo y de Calidad, asegura el correcto funcionamiento de los diferentes procesos administrativos como también de la calidad en la prestación de los servicios de seguridad y vigilancia. Define los recursos tanto materiales como humanos para dar cumplimiento con la misión institucional y realiza seguimiento de las licitaciones y cotizaciones presentadas. Ejerce control sobre sucursales y agencias, se ocupa de la atención y servicio al cliente. Además son responsables de cumplir con las disposiciones legales propias de la naturaleza del servicio.

Organismo de Recurso Humano, vela por el buen desempeño del recurso humano, garantiza la contratación de personal que cumpla con los perfiles establecidos, integra el comité disciplinario, toma la decisión de contratación de nuevo personal en el área operativa y administrativa, coordina el programa de salud ocupacional.

Organismo Operativo, es el responsable de ejecutar el servicio con calidad en forma oportuna, controla el movimiento de armas, radios, relojes, salvoconductos y trabajo de los supervisores. Organizan turnos y ubican al personal en los puestos de trabajo, apoyan en forma directa el proceso de nomina.

4.1.3 Descripción del entorno informático

En este apartado remitimos al lector al Anexo C Configuración del Sistema Informático de Sevicol Ltda., donde se describe los recursos que forman parte del entorno informático de la empresa.

4.1.4 Selección de los recursos del entorno informático a auditar

Tratando de dar la mayor cobertura que una auditoria puede alcanzar, se auditaran los recursos de tecnología de la información identificados por el modelo COBIT dentro del marco aceptado de Control Interno Informático como

se explico en el capitulo 2. Haciendo énfasis en los procesos que se identificaron como vitales (Nomina, Facturación, Cartera y Contabilidad).

4.1.2 ESTUDIO DE RIESGOS

4.1.2.1 Definición de los riesgos a estudiar

Como hemos mencionado nuestro trabajo de auditoria esta orientado en la identificación de los riesgos asociados por el uso de tecnologías de la información que apoyan los procesos administrativos y operativos en la empresa y que puedan afectar los requerimientos de la información sugeridos en el modelo COBIT. Lo que sugiere una definición de riesgo propia a aplicarse en el presente trabajo así:

> *Riesgo es la probabilidad que ocurra un evento que ocasione un impacto no deseado sobre los requerimientos de la información que están asociados con el uso de tecnologías de la información (TI).*

Algunos daños a los requerimientos de la información son los siguientes:

Tabla 4.1 Posibles daños que genera el acontecimiento de un riesgo

Requerimiento de Información	Daño
Integridad	Carencia de precisión y suficiencia de la información, así como a su invalidez de acuerdo con los valores y expectativas del negocio.
Confiabilidad	Provisión de información inapropiada para la administración o dirección del negocio.
Confidencialidad	Especifica la falta de protección a la información sensible contra divulgación no autorizada.
Disponibilidad	Se refiere a la limitación de obtener la información cuando esta es requerida.
Cumplimiento de leyes y regulaciones	Sanciones por incumplimiento de las leyes y regulaciones propias al ejercicio del servicio prestado.
Efectividad	Señala la inconveniente e inapropiada información que posee la administración para la toma de decisiones.
Eficiencia	Significa la inmediatez con que la información puede ser obtenida utilizando los recursos de manera optima y económica.

4.1.2.2 Identificación de los riesgos

La identificación de los riesgos es el señalamiento de la situaciones presentes en el entorno informático que pueden causar daño a los requerimientos de la información. Para tal fin y como forma de organizarlos, se clasifican los riesgos de acuerdo al recurso de TI que este siendo auditado.

4.1.2.3 Construcción del sistema de valoración de riesgos

Esta técnica permite recolectar en forma sistemática y organizada la información detallada sobre la identificación, localización y valoración de los riesgos asociados con el uso de tecnologías de la información. Dentro de este sistema de valoración de riesgos se hace necesario incluir ciertas variables que permitan determinar el grado de peligrosidad de los riesgos, objetivo primordial para diseñar las acciones preventivas para reducir o disipar sus efectos. Estas variables son:

- Probabilidad de ocurrencia de un riesgo
- Medidas de impacto del riesgo sobre los requerimientos de la información
- Materialidad y grado de peligrosidad del riesgo
- Recurso de TI que esta siendo afectado

4.1.2.4 Cálculo de la probabilidad

Debido a la inexistencia de datos estadísticos acerca de la probabilidad de la manifestación de los riesgos identificados, se ha recurrido a la opinión de los expertos, que en este caso son las personas que directamente trabajan sobre el entorno informático de la empresa.

Estas personas que deben tener un criterio lo más objetivo posible, se identificaron fácilmente, debido al conocimiento que se ha obtenido de la empresa, producido en la etapa preliminar de la metodología.

Luego de haber identificado a las personas, se les hace entrega de una lista de riesgos donde consignan su juicio valorativo. En este punto, es necesario aclarar que pueden existir varias listas para un determinado grupo de riesgos y de personas. El número de personas que analizarán cada grupo de riesgos para este caso será de tres asesorados en forma directa por el auditor.

Cada persona asignará un valor ente 0 y 100 a cada riesgo identificado como manera de evaluar su probabilidad de ocurrencia.

4.1.2.5 Medida del impacto del riesgo sobre los requerimientos de la información

Luego de haber asignado la probabilidad a cada riesgo, se procede a establecer cual será su impacto sobre cada una de las características de la información en el caso en que este llegará a manifestarse. El valor del impacto será un número comprendido entre 1-10 como se explica en la siguiente tabla:

Tabla 4.2 Medida del impacto sobre los requerimientos de la información

Grado del Impacto	Valores
Bajo	0-3
Medio	4-7
Alto	8-10

4.1.2.6 Materialidad y grado de peligrosidad del riesgo

Una vez establecido el impacto sobre cada uno de los requerimientos de la información, la materialidad de cada riesgo, se define como la sumatoria de los valores asignados y finalmente, el grado de peligrosidad como la multiplicación de la materialidad por la probabilidad.

4.1.2.7 Lugar donde el riesgo se puede manifestar

Para nuestro interés, el lugar donde se puede manifestar el riesgo es directamente el recurso que este siendo auditado el cual se identifica en la primera columna de nuestra matriz.

4.1.2.8 Valoración de riesgos

Tabla 4.3 Valoración de riesgos en materia de Control Interno Informático

Proceso	Número	Riesgo	Impacto							Valoración		
			Integridad	Eficiencia	Efectividad	Disponibilidad	Cumplimiento	Confidencialidad	Confiabilidad	Materialidad	Probabilidad	Grado de Peligrosidad
Organización general del Servicio Informático	1	Ausencia de un comité de informática, responsable de las principales decisiones estratégicas.	7	7	6	7	7	5	5	44	80	35.2
	2	Ausencia de un plan de informática	7	8	8	8	6	5	8	50	80	40.0
	3	Falta una persona encargada de auditar la gestión de la función informática	3	7	4	4	7	4	3	32	40	12.8
	4	Se considera en el diseño de nuevas aplicaciones los problemas emanados por el uso y con la adecuación de procedimientos administrativos	5	7	5	7	8	6	6	44	70	30.8
	5	No existe separación entre las funciones de explotación y desarrollo	5	8	5	6	5	5	4	41	70	28.7
	6	Dependencia del personal de informática y utilización de métodos y software poco utilizados	7	8	9	6	8	5	5	48	75	36.0
	7	Falta de un procedimiento técnico para adquirir soluciones informáticas	8	8	6	6	9	5	5	49	85	41.65
Desarrollo y Mantenimiento de Software	8	Ausencia de una metodología de desarrollo de aplicaciones, incluido un estudio previo de oportunidad	4	7	5	4	6	4	3	33	50	16.5
	9	Se analizan las ventajas e inconvenientes de la adquisición de un programa o la realización de un sistema especifico	7	8	7	8	4	6	4	44	85	37.4
	10	Ausencia de normas relativas al contenido de los archivos al momento de nombrarlos	7	8	8	7	8	3	5	46	85	39.1

Proceso	Número	Riesgo	Impacto							Valoración		
			Integridad	Eficiencia	Efectividad	Disponibilidad	Cumplimiento	Confidencialidad	Confiabilidad	Materialidad	Probabilidad	Grado de Peligrosidad
Desarrollo y Mantenimiento de Software	11	Esta previsto en el desarrollo de nuevas aplicaciones las principales fases de puesta en marcha de un proyecto	7	8	8	6	9	5	4	47	80	37.6
	12	Ausencia de un seguimiento y coordinación de los proyectos informáticos	5	8	6	8	5	8	6	47	40	18.8
	13	Falta de políticas de calidad que gobiernen la función informática	7	9	7	5	7	4	7	46	70	32.2
	14	Falta de documentación de las aplicaciones o no es satisfactoria	8	8	6	7	5	4	4	42	80	33.6
	15	Ausencia o presencia no adecuada de procedimientos de mantenimientos de software	8	8	5	8	8	6	5	48	75	36.0
Entorno de Producción	16	No existe biblioteca de programas fuentes	7	8	7	7	8	5	5	47	90	42.3
	17	Ausencia o presencia ineficiente de una política de control interno en los procedimientos de toma de datos	7	8	7	7	7	5	8	49	70	34.3
	18	Ausencia de procedimientos de recuperación de aplicaciones en explotación en caso de incidentes	7	8	5	5	9	4	4	42	50	21
	19	Ausencia de controles de seguridad y seguimiento a los usuarios	5	6	4	8	8	7	7	45	80	36
	20	Deficiencia en el seguimiento de la calidad de los servicios suministrados por informática	5	8	4	7	8	5	6	43	70	30.1
	21	Proliferación en disco de archivos inútiles o que no respeten una estructura definida previamente	5	8	7	6	5	7	7	45	80	36

Proceso	Número	Riesgo	Impacto							Valoración		
			Integridad	Eficiencia	Efectividad	Disponibilidad	Cumplimiento	Confidencialidad	Confiabilidad	Materialidad	Probabilidad	Grado de Peligrosidad
Entorno de Producción	22	Ausencia de bibliotecas de programas, centro de mantenimiento y de documentación	7	8	5	6	8	5	5	44	75	33
	23	Permiten las copias de seguridad en un plazo satisfactorio resolver todo tipo de fallos?	7	8	7	8	8	5	7	50	75	37.5
	24	Deficiencia en el procedimiento de copias de seguridad en el conjunto software y archivos necesarios para desarrollo y explotación	7	8	8	8	7	7	7	52	75	39
	25	Existen backups en un sitio diferente a la empresa para recuperar el funcionamiento en caso de siniestros	7	8	8	8	8	7	7	53	85	45.05
	26	Ausencia de un programa de reinicio de operaciones en caso de siniestro	6	8	8	6	9	5	5	47	80	37.6
	27	Acceso no autorizado al cuarto del servidor	4	8	5	7	5	7	7	43	75	32.25
	28	Evaluación de controles sobre incendios, inundaciones, interrupciones eléctricas e intrusos	4	7	5	7	7	7	4	41	60	24.6
Funciones de Asistencia Técnica	30	¿Hay un administrador de Datos?	6	6	4	6	6	5	5	38	70	26.6
	31	¿Se utiliza diccionario de datos?	6	6	4	6	6	5	5	38	65	24.7
	32	¿Se procura optimizar la base de datos?	4	7	5	6	5	6	6	39	75	29.25
	33	Existe un encargado de la seguridad en el departamento de sistemas?	5	7	6	7	7	8	5	45	75	33.75
	34	Falta de un plan de seguridad informática	4	7	6	6	8	7	5	43	65	27.95

Tabla 4.4 Auditoría de: Instalaciones, Seguridad Física y Lógica

Proceso	Número	Riesgo	Impacto							Valoración		
			Integridad	Eficiencia	Efectividad	Disponibilidad	Cumplimiento	Confidencialidad	Confiabilidad	Materialidad	Probabilidad	Grado de Peligrosidad
Auditoria de: Instalaciones, Seguridad Física y Logia	35	Aumento de costos y subestimación de recursos por falta de una evaluación de sistemas existentes	5	7	6	6	5	6	5	40	60	24
	36	Perdidas asociadas a la sede por falta de adecuación para soportar recursos tecnológicos	3	5	4	7	7	7	5	38	40	15.2
	37	Traumatismo en el reinicio de operaciones por desastre al no contar con plan de contingencias	8	9	7	5	7	5	5	46	90	41.4
	38	Daños y perdidas por falta de un responsable de seguridad física y lógica que dirija y capacite al personal	5	7	6	7	7	7	4	43	65	27.95
	39	Tiempo de respuesta no apropiado por parte de soporte técnico y mantenimiento	4	6	6	5	8	8	6	43	35	15.05
	40	Recurrencia de problemas e incidentes por una no adecuada técnica de administración de los mismos	6	8	7	6	5	5	6	43	80	34.4
	41	Perdida de disponibilidad de recursos por fallas físicas, asignación no equitativa y prioridades de tarea	4	7	4	5	7	5	4	36	50	18
	42	Perdida de información por uso no autorizado, divulgación, modificación daño o perdida	4	7	4	7	7	4	3	36	50	18
	43	Ausencia de un documento de configuración del sistema que permita conocer y controlar detalladamente el entorno informático	7	7	6	7	7	8	5	47	75	35.25

Tabla 4.5 Auditoría de Datos

Proceso	Número	Riesgo	Impacto							Valoración		
			Integridad	Eficiencia	Efectividad	Disponibilidad	Cumplimiento	Confidencialidad	Confiabilidad	Materialidad	Probabilidad	Grado de Peligrosidad
Auditoria de Datos	44	Formas de entrada de datos no adecuadas perjudicando la integridad de los mismos	5	6	4	7	4	7	7	40	40	16
	45	Revisión no detallada de documentos fuentes por personal de confianza antes de ser ingresado al sistema	6	7	6	8	5	5	5	42	60	25.2
	46	Deficiencia en asegurar la calidad de los documentos fuentes en cuanto a precisión, que sean completos y transmitidos oportunamente	7	7	5	3	3	4	5	34	40	13.6
	47	Se puede asegurar que la entrada de datos y actualización es llevada a cabo por personal autorizado	5	5	3	8	8	4	8	41	40	16.4
	48	Errores por una deficiente validación y edición de datos en los sistemas	8	7	7	7	6	4	4	43	70	30.1
	49	Perdida de información por manejo poco seguro, acceso no autorizado o modificación	4	8	5	8	8	4	8	45	30	13.5
	50	No son adecuados los procedimientos de almacenamiento de datos	7	7	4	7	8	7	4	44	35	15.4
	51	Se consideran confiables los procedimientos para controlar errores en la salida de datos: Balanceo y conciliación	5	8	4	8	7	7	8	47	25	11.75
	52	Segregación de funciones no apropiada y poco control del trabajo en proceso que repercute en el flujo de errores	6	8	5	6	5	5	4	39	60	23.4

Tabla 4.6 Auditoria de Aplicaciones según el enfoque de Price Waterhouse

Proceso	Número	Riesgo	Impacto							Valoración		
			Integridad	Eficiencia	Efectividad	Disponibilidad	Cumplimiento	Confidencialidad	Confiabilidad	Materialidad	Probabilidad	Grado de Peligrosidad
Acceso a Funciones de Procesamiento	53	Acceso de personas no autorizadas a funciones del software, permitiéndoles: leer, modificar, agregar y eliminar datos	8	7	7	8	8	5	8	51	25	12.75
	54	Ausencia de pistas de auditoría que permitan hacer seguimiento a las transacciones	5	6	4	7	6	5	6	39	60	23.4
	55	El sistema no tiene módulos donde se manejen funciones por separado y restrinjan el acceso solo a usuarios autorizados	4	8	4	7	5	5	8	41	75	30.75
	56	Actualización de archivos por personas no autorizadas o corridas no programadas	5	8	7	7	4	3	5	39	75	29.25
Ingreso de Datos	57	El formato de los campos no restringe el ingreso de datos que no corresponden al formato especificado	7	7	6	7	5	3	3	38	75	28.5
	58	Las aplicaciones en sus formas aceptan campos en blanco	8	9	5	5	4	4	7	42	80	33.6
	59	No existen limites razonables en los campos numéricos, algunos aceptan hasta 10 cifras	8	9	5	8	5	5	6	46	75	34.5
	60	No hay comparación con datos existentes en el sistema al momento de su registro. Ej.SMLV	8	9	6	9	4	7	7	50	80	40
	61	Existen archivos que permiten la existencia de datos duplicados E.j.SMLV	7	8	7	9	4	5	8	48	80	38.2

Proceso	Número	Riesgo	Impacto							Valoración		
			Integridad	Eficiencia	Efectividad	Disponibilidad	Cumplimiento	Confidencialidad	Confiabilidad	Materialidad	Probabilidad	Grado de Peligrosidad
Ingreso de Datos	62	Deficiencia en la correlación de campos	7	8	7	8	3	7	7	47	75	35.25
	63	Escasa documentación donde se describa los atributos de los campos y la información que estos puedan requerir	7	8	5	6	4	3	6	39	75	29.25
Items rechazados o en suspenso	64	Interrupción abrupta de un proceso en ejecución por falla en fluido eléctrico, generando perdida de tiempo e información	8	8	6	7	7	4	4	44	75	33
	65	No existen procedimientos de recuperación lo que obliga a ejecutar toda la operación	7	7	4	7	7	3	3	38	60	22.8
Procesamiento	66	Algunas transacciones pueden ser registradas y ejecutadas en un periodo contable diferente al actual	7	7	5	8	7	4	8	42	80	33.6
	67	En caso que el sistema falle se debe esperar hasta su reparación. No existen equipos de respaldo	6	8	7	5	9	3	4	42	75	31.5
Estructura Organizativa	68	Deficiencia en la estructura organizacional de sistemas lo que no permite administrar eficientemente este recurso	4	8	3	4	3	7	6	35	60	21.0
	69	Ausencia de autorización de corridas no programadas	8	8	7	7	6	6	5	47	60	28.2
	70	Deficiencia en la documentación de manuales de operaciones y aplicaciones	3	8	5	5	7	3	3	34	65	22.1

Proceso	Número	Riesgo	Impacto							Valoración		
			Integridad	Eficiencia	Efectividad	Disponibilidad	Cumplimiento	Confidencialidad	Confiabilidad	Materialidad	Probabilidad	Grado de Peligrosidad
Cambios a los Programas	71	No existen procedimientos de documentación de cambios hechos en los programas	4	6	6	6	7	3	3	35	75	26.25
	72	No hay división entre el área de producción y explotación de software	5	8	7	7	6	7	4	44	75	33
	73	El mantenimiento de los programas se realiza directamente sobre las aplicaciones en funcionamiento. No existen procedimientos adecuados	6	8	9	6	5	5	4	43	75	32.25
	74	No hay registro de las versiones de los programas, no existe control de crecimiento del sistema	6	9	8	6	6	7	3	45	80	36
Acceso general	75	El cuarto del servidor es de fácil acceso y no se restringen y controlan las entradas	4	7	5	8	6	4	7	41	55	22.55
	76	No existen procedimientos de validación y cambios de usuarios y contraseñas	5	8	5	8	7	4	7	41	60	24.6

Tabla 4.7 Valoración de riesgos para Tecnologías de la información

Proceso	Número	Riesgo	Impacto							Valoración		
			Integridad	Eficiencia	Efectividad	Disponibilidad	Cumplimiento	Confidencialidad	Confiabilidad	Materialidad	Probabilidad	Grado de Peligrosidad
Aspectos generales para Tecnologías de la Información	77	Ausencia de documentación sobre características físicas y lógicas de la red	3	5	4	7	7	3	5	34	35	11.9
	78	Acceso a Internet via MODEM sin medidas de seguridad adecuadas	5	6	6	5	7	4	8	41	75	30.75
	79	Ausencia de un documento que describa el inventario de hardware y software de la Cia.	3	6	4	7	7	3	6	36	35	12.6
	80	Escasa preparación del personal en el manejo de tecnologías de información	5	6	4	6	4	4	6	35	75	26.25
	81	Los documentos importantes o privados para cada equipo no poseen contraseña para acceso en red.	6	7	5	7	5	8	7	45	75	33.75
	82	Deficiencias en las copias de seguridad de archivos en puestos de trabajo	4	7	5	7	4	4	6	37	60	22.2
	83	Desaprovechamiento de los recursos y/o avances tecnológicos con que cuenta la _Cia.	3	7	5	5	4	3	6	33	50	16.5

4.1.2.9 Jerarquización de los riesgos

Esta etapa, a partir del análisis y evaluación de los riesgos identificados y de una escala de indicadores que se presentara a continuación, permite orientar el trabajo a seguir por parte del auditor en la elaboración y ejecución de pruebas y en el diseño e implementación de controles de la siguiente forma:

- Elaboración de pruebas: sobre los riesgos identificados para comprobar su manifestación o deficiencias en los controles establecidos.

- Diseño e implementación de controles priorizando su ejecución dependiendo del grado de peligrosidad identificado en la matriz de valoración de riesgos:

Tabla 4.8 Intervalos de tiempo para el diseño e implementación de controles

Plazo para el diseño e implementación de controles	Grado de peligrosidad (ptos)
Inmediato	37-46
Corto Plazo	28-36
Mediano Plazo	19-27
Largo Plazo	12-18

4.1.2.10 Priorización para el diseño e implementación de controles

Debido a la dirección del presente trabajo de Auditoria en materia de control interno informático (en cuanto a lo que se trato en el estudio de riesgos) y reconociendo que SEVICOL LTDA, no cuenta con un procedimiento de control de su recurso tecnológico, en este punto se recomienda priorizar el diseño e implementación de controles orientado a construir un manual de control interno informático aceptado y adecuado a las necesidades de la compañía de la misma forma como se planteo en el estudio de riesgos.

4.2 ETAPA DE ELABORACIÓN Y EJECUCIÓN DE PRUEBAS

4.2.1 DESCRIPCION DEL AMBIENTE DE CONTROL DE SEVICOL LTDA.

Debido a la naturaleza del servicio que presta SEVICOL y a las características sociales de nuestro país, en materia de seguridad, la empresa ha presentado un aumento considerable en el número de clientes, en su personal operativo y por ende el volumen de información a administrar.

Este crecimiento de la empresa igualmente ha contribuido en el mejoramiento de su personal que día a día, ha pasado de cargos elementales a cargos de control y mayor responsabilidad, debido al conocimiento que tienen del negocio y la confianza de la cual han sido merecedores.

Lo anterior permite concluir en una descripción de un ambiente de control organizacional caracterizado por la confianza, donde cada persona conocedora y responsable de su función se encarga de llevarla a cabo ejecutando rutinas de control, aunque no documentadas, si implícitas en los procesos. Usuarios con todos los permisos y derechos para acceder los SI que en algunos casos conlleva a cometer errores involuntarios en procesos que no son de su competencia o redundancia en el ejercicio de sus funciones. Este ambiente organizacional, conlleva a configurar un control interno informático no documentado sin un responsable de hacerlo cumplir o mejorarlo.

Por supuesto, lo hecho hasta el momento en la Cía. en materia de control interno informático ha sido funcional alcanzando los objetivos definidos para cada proceso que es apoyado por informática a través de controles tales como revisiones, firmas, conteos y comparaciones.

Tabla 4.9 Controles establecidos en los procesos del SI

No.	Nombre del Control	Descripción
1	Control previo a firma	Comprende la revisión de documentos antes de ser firmados por los responsables. Se realiza con el fin de detectar inconsistencias en los documentos implicados en la revisión.
2	Control de comparación	Se presenta cuando en 2 o más documentos se comparara información textual y/o numérica a fin de establecer coincidencias y posibles diferencias.
3	Revisión de diligenciamiento	Es la revisión que se hace de uno o más documentos para verificar que el contenido del mismo corresponde a lo esperado. No precede a una acción de firma.
4	Control por conteo	Cuando se trata de verificar cantidades de documentos, objetos o dinero en desarrollo de un proceso.
5	Control por confirmación personal	Cuando se verifica: información, cumplimiento de diligencias, trámites, deudas, etc., a partir del contacto directo con el responsable.

4.2.2 DISEÑO Y APLICACIÓN DE PRUEBAS

En las dos siguientes tablas se presentan el tipo de prueba que se puede ejecutar para verificar el cumplimiento de controles establecidos (pruebas de cumplimiento) o evidenciar la ausencia de los mismos (pruebas sustantivas) con un correspondiente mnemónico para recordar el tipo de prueba efectuada.

Tabla 4.10 Pruebas de cumplimiento

ID Prueba	Procedimiento	Descripción
C1	Indagación	Prueba testimonial que efectúa el auditor con el fin de confirmar si el personal conoce y aplica los controles y procedimientos que debe realizar en sus actividades
C2	Manifestación	Prueba testimonial que presenta por su propia voluntad el personal al auditor, comentando las deficiencias y mejoras de los mecanismos de control en los procesos del SI
C3	Observación	Prueba visual que efectúa el auditor sobre el flujo de actividades de algún proceso con el objetivo de confirmar la ejecución de los controles.
C4	Inspección de Documentación	El auditor inspeccionará directamente los diferentes documentos que intervienen en los procesos, para identificar, si posee las firmas necesarias, su diligenciamiento es correcto, y si la información consignada es la esperada.

Tabla 4.11 Pruebas Sustantivas

ID Prueba	Procedimiento	Descripción
S1	Indagación	Prueba testimonial que efectúa con el fin de confirmar si el personal percibe y es consciente de la manifestación de los riesgos en sus actividades.
S2	Observación	Prueba visual que comete el auditor sobre el flujo de actividades de algún proceso con el objetivo de confirmar la manifestación de los riesgos.
S3	Análisis	Prueba analítica donde el auditor examina el comportamiento de una variable frente a un comportamiento esperado y razonable utilizando cálculos o chequeo de la precisión matemática.
S4	Transaccionales	Prueba que ejecuta el auditor para corroborar con total certeza la validez de una transacción o la veracidad de un saldo lo cual se puede hacer a través de: inspección de documentos y registros soportes, inspección física de los objetos, confirmación externa con el sujeto generador de la transacción y reproducción o reejecución de la transacción
S5	Inspección de documentación	Se inspecciona los formatos de consignación de información en la documentación existente, con el fin de encontrar fallas en su estructura y contenido.

4.2.2.1 Aplicación de pruebas y consignación de resultados

En esta parte utilizamos tablas que describen de la siguiente manera el procedimiento efectuado asi:

La primera columna identifica el riesgo, de acuerdo al número asignado en el estudio de riesgos. La siguiente columna contiene el objetivo de la prueba asociado al riesgo en estudio, la tercera columna identifica el tipo de prueba como se definió en las tablas 4.10 y 4.11. La cuarta columna el procedimiento realizado en la prueba. La quinta columna registra el resultado obtenido luego de aplicar la prueba.

4.2.2.2 Pruebas sustantivas y de cumplimiento en materia de control interno informático

Tabla 4.12 Pruebas a la Organización del Servicio Informático

ID Riesgo	Objetivo	ID Prueba	Procedimiento especifico de la prueba	Resultados
1	Evidenciar la necesidad de definir un comité de informática	S1	¿El organismo directivo reconoce la importancia de definir dicho comité?	Si, y en ocasiones lo han propuesto a nivel de junta, pero no lo han llevado a la practica.
		C1 C2	¿Los ing. Responsables de Informática cumplen su labor?	Si, aunque cada uno tiene definida su función, en ocasiones presentan retrasos en su atención debido a otras responsabilidades deferentes de sistemas. El ing. Jefe manifestó que sus múltiples ocupaciones no le permiten atender de la mejor manera el recurso informático.
2	Evidenciar la importancia de definir un plan de informática	S1	¿Los responsables de informática reconocen la importancia de definir dicho plan?	Si, y reconocen que es vital para el progreso tecnológico de la compañía.
		C1	¿Comprobar dentro del proyecto e inversión trimestral en tecnología si es ejecutado?	No como se convino, al inicio se cumplió pero luego se descuido y las inversiones son de carácter correctivo
3	Demostrar la necesidad de un encargado de gestión de la función informática	S1	Analizar con los responsables de informática que tan necesario es este rol	Se concluye que si es importante ya que esta persona velaría pro el funcionamiento eficaz y eficiente de este departamento.
		S2	Verificar que por falta de un responsable de informática se generan traumatismos	Con frecuencia se producen errores repetivos que hacen perder tiempo a los operarios al no ser consignados y corregidos.

ID Riesgo	Objetivo	ID Prueba	Procedimiento especifico de la prueba	Resultados
4	Confirmar si los responsables de informática adecuan los SI de acuerdo a los requerimientos del negocio	S1	El personal usuario de SI es atendido cuando se hace necesario un ajuste o mejoramiento del SI	Si, normalmente los ing. Encargados modifican los programas para satisfacer la necesidades del proceso.
		S2	Comprobar las mejoras que son realizadas al SI.	Aquí se pode de manifiesto que aunque los SI se adecuan a las necesidades no son objeto de un control de crecimiento los arreglos son fruto de la necesidad.
5	Comprobar que no hay separación de funciones entre desarrollo y explotación	S1	Se entrevisto al ing. Jefe sobre los programas fuentes y su mantenimiento	El ing. Manifiesta que no hay fuentes es decir las mejora se hacen sobre el software instalado y en uso, no hay versiones anteriores y su crecimiento no hay sido controlado.
6	Demostrar la dependencia al utilizar software y métodos poco difundidos	S1	Recoger opiniones de desarrolladores de software sobre DataEase	Manifiestan que es una herramienta de muy fácil manejo y poco exigente, facil de aprender, pero tiene desventajas al estar sujeta al DOS y esta muy poco difundido
		S2	Verificar utilización de métodos no adecuados de desarrollo	Se comprueba que la aplicación de nomina no esta normalizada
7	Mostrar la necesidad de estructurar un modelo de inversión en soluciones tecnológicas	S1	Realizar entrevistas para comprobar deficiencias en este aspecto al personal ejecutivo	Se muestran de acuerdo en formalizar un modelo de inversión donde se definan formas de cómo proteger la empresa por incumplimiento de proveedores.

Tabla 4.13 Pruebas al Desarrollo y Mantenimiento de Software

ID Riesgo	Objetivo	ID Prueba	Procedimiento especifico de la prueba	Resultados
8	Confirmar si los jefes de informática conocen y aplican una metodología de desarrollo de software	S1	Los ing. Responsables de informática son consientes de la necesidad de definir y seguir una metodología de desarrollo de software	Si, aunque en la actualidad no se ha hecho desarrollo, manifiestan preferir el modelo de ciclo de vida tal como se hizo cuando se diseño el SI original.
9	Demostrar la necesidad de implementar un modelo de inversión e implementación de aplicaciones	S1	Realizar entrevistas a los responsables de informática	Los ing. Manifiestan que aunque no esta definido en documento un modelo tal, si se sigue un procedimiento de inversión para proteger la empresa contra incumplimientos de proveedores.
		C2	Confirmar con el personal usuario sobre la forma de realizar las inversiones en informática.	En general, todos reconocen que los SI hacen lo que se le pide pero no es eficiente, algunos sugieren que ya es hora de implementar algo nuevo. Recurso humano manifestó que cuando se adquirió una aplicación de manejo de personal su puesta en marcha fue lenta y no había soporte oportuno.
10 21	Necesidad de definir normas para nombrar archivos y su ubicación	S1	El personal usuario es consiente de definir buenas practicas para nombrar archivos	Si, y así lo hacen aunque usan un método no muy eficiente

ID Riesgo	Objetivo	ID Prueba	Procedimiento especifico de la prueba	Resultados
11	Necesidad de definir buenas prácticas en las fases de puesta en marcha de proyectos informáticos	S1	Los jefes de sistemas son consientes de la necesidad de definir buenas prácticas para las fases de puesta en marcha de nuevos proyectos	Si, y siguen algunas fases aunque no están documentadas.
14	Verificar que tan adecuada es la documentación de las aplicaciones	S5	Se revisa y se utiliza para saber que tan apropiada es.	La documentación existente ayuda a los usuarios en el funcionamiento de las aplicaciones por el conocimiento que tienen, pero no esta completa.
15	Comprobar que tan adecuados son los procedimientos de mantenimiento de software	S2	Se observa en el transcurso de la Auditoría como hacen el mantenimiento al SI.	El mantenimiento es de tipo correctivo es decir, de acuerdo a las necesidades, los archivos maestros contienen información no necesaria de periodos anteriores. Además, se realiza sobre las aplicaciones en marcha.

Tabla 4.14 Pruebas al Entorno de Producción

ID Riesgo	Objetivo	ID Prueba	Procedimiento especifico de la prueba	Resultados
16 22	Evidenciar la necesidad de construir una biblioteca de programas y mantener copias en lugar diferente a la empresa	S1	Se cuestiona a los ing. Responsables que procedimiento seguir en caso fallas en la prestación del servicio por desastre o atentados	Manifiestan que seria grave si algo así sucediera, aunque cuentan con copias de datos no así de las aplicaciones lo que provocaría traumatismos serios en la continuidad del servicio.
17	Evidenciar algunas deficiencias en el ingreso de datos	S5	Verificar que los formatos de datos sean validos	Algunos datos de formato numérico aceptan texto.
18 19 25 26,37	Necesidad de definir un plan adecuado de contingencias	S1	Se cuestiona a los jefes de sistemas que hacer en caso de desastre o atentados	Reconocen que seria traumático el reinicio de operaciones del servicio informático al no existir un plan de contingencias adecuado.
23 24	Verificar que tan adecuados son las copias de seguridad en el conjunto datos y aplicaciones	S1	Los jefes de sistemas están conformes con las copias de seguridad del conjunto datos y aplicaciones	No, se concluye que aunque está definido un procedimiento de copia de seguridad de datos semanalmente no se ejecuta con rigor, y no hay copias de programas fuentes.
27	Verificar acceso al cuarto del servidor	C3	Observar quienes acceden el cuarto del servidor	Existen controles de ingreso, avisos de advertencia y puerta cerrada permanentemente pero no esta definido quienes pueden o no accederlo.
28 36	Verificar los controles en el edificio sobre incendios, inundaciones e intrusos	C3	Revisar los mecanismos establecidos para controlar estos riesgos	En materia de seguridad cuentan con los controles adecuados, detectores de humo de movimiento, equipos contra incendios y entrenamientos en caso de siniestro, pero deberían ser más estrictos con el ingreso de personal

Tabla 4.15 Pruebas a las Funciones de Asistencia Técnica

ID Riesgo	Objetivo	ID Prueba	Procedimiento especifico de la prueba	Resultados
30 31 32	Necesidad de nombrar un administrador de la BD y definir funciones	S1	Los jefes de sistemas son consientes de la necesidad de administrar eficientemente la BD.	Si, pero no disponen de tiempo suficiente para hacerle seguimiento y adecuarla.
33 34 38 42	Evidenciar la necesidad de nombrar un encargado de seguridad informática o al menos algunas funciones	S1	Los jefes de sistemas reconocen necesidad de definir información confidencial y demás normas de seguridad informática y proteger los datos contra errores voluntarios e involuntarios	Si, y lo manifestaron además sugieren que dentro de las recomendaciones se le de prioridad a la seguridad de entorno informático.

Tabla 4.16 Pruebas a las instalaciones: Seguridad Física y Lógica

ID Riesgo	Objetivo	ID Prueba	Procedimiento especifico de la prueba	Resultados
35 43	Conocer el potencial tecnológico y humano con que cuenta la cía.	S5	Revisar los inventarios de tecnologías y actualizarlos para poder evaluar dicho recurso.	La empresa cuenta con un recurso tecnológico adecuado y de última generación pero no aprovechado al máximo.
39 41	Evidenciar la necesidad de adecuar los servicios técnicos de mantenimiento mas eficientemente	S1	Los usuarios están conformes con el mantenimiento de equipos	No, además argumentan que los hacen en oras laborales interrumpiendo el normal funcionamiento, igualmente no son oportunos y tardan en acudir a solucionar problemas.

Tabla 4.17 Pruebas de Auditoria de Datos

ID Riesgo	Objetivo	ID Prueba	Procedimiento especifico de la prueba	Resultados
44 57 58 59	Demostrar deficiencias en el ingreso de Datos	S5	El formato del dato es el formato correcto en el campo de la BD	El tipo de dato del mayor número de campos no cumple con el formato que debería tener.
		S3	El SI permite que datos importantes queden faltantes	Si, son pocos los datos que son considerados necesarios para completar transacciones
		S3	Verificar control de limites para datos numéricos	No existen limites razonables en los campos numéricos, algunos aceptan hasta 10 cifras.
45 46	Comprobar validez de los datos antes de ingresar al sistema	S1	Asegurar la revisión de listas de datos por personal de confianza antes de ser actualizados en el sistema	Los datos son ingresados por los usuarios, luego se imprimen listas de verificación y se corrige para imprimir y actualizar finalmente pero no son revizados por algún ejecutivo.
47	Verificar si la actualización del SI es llevado a cabo por personal autorizado	C1	Conocer y observar la persona encargada de realizar la actualización del SI.	La Auxiliar contable es la persona encargada de llevar proceso de actualización de maestro cuando lo ejecuta lo comunica a los demás usuarios.

ID Riesgo	Objetivo	ID Prueba	Procedimiento especifico de la prueba	Resultados
48 66	Verificar calidad en cuanto edición y validación de datos del SI	S3	Se hace copia de la aplicación nomina y se realizan diferentes operaciones	Aun cuando existe una forma de constantes de nomina donde se define SMLV cuando se enra a liquidar un sueldo se puede modificar este valor en el campo correspondiente.
		C2	Comprobar si se puede trabajar periodos contables diferentes al actual	Si, y en una ocasión se registro una factura son fecha de un año superior y el sistema lo valido.
49	Demostrar los riesgos que corre la información por manejo no adecuado	S1	Se entrevistan usuarios y se recoge su opinión	Un usuario manifestó que en una ocasión se periodo la información de nomina de un periodo por interrupción eléctrica en el momento de actualización del movimiento
51	Confirmar el funcionamiento de los controles de verificación de saldos, y liquidación de nomina	C3	Se acompaña a los usuarios en el proceso de conciliación y verificación de liquidación de nomina	El procedimiento es adecuado y efectivo aunque presenta fallas por falta de concentración de los operarios por atención de otras actividades.

Tabla 4.18 Pruebas de Auditoria a las Aplicaciones

ID Riesgo	Objetivo	ID Prueba	Procedimiento especifico de la prueba	Resultados
53 56	Verificar si personas no autorizadas accesan el SI.	S2	Se observan los usuarios al manipular el SI.	Debido al ambiente de control de la Cía., todos los usuarios tienen permisos y acceso a todas las funciones del SI. El riesgo puede ser resultado de una mala operación de las aplicaciones de carácter voluntario e involuntario.
54	Evidenciar necesidad de implementar pistas de Auditoria	S1	Entrevistar jefes de sistemas y tomar su opinión al respecto.	El ing., manifiesta que en ocasiones cuado un usuario comete un error y no lo reconoce este se pone en la tarea de averiguar que y como se produjo el error provocándole perdida de tiempo al no existir procedimiento de reconstrucción y seguimiento de transacciones.
		C4	Revisar el control de registro de ultimo usuario en utilizar el recurso	Este control almacena el nombre de usuario y equipo del usuario que utiliza una aplicación eficientemente.
55	Demostrar la necesidad de rediseñar menús que restrinjan el acceso a cualquier procedimiento del SI.	S5	Se explora el SI y se accesan los procesos disponibles ejecutando algunas operaciones	Se comprueba que todos los procesos del SI están disponibles para cualquier usuario con posibilidad de ejecutarlos en cualquier momento, no existen módulos donde se manejen y restrinjan las funciones por separado

ID Riesgo	Objetivo	ID Prueba	Procedimiento especifico de la prueba	Resultados
60	Comprobar la funcionalidad de datos constantes definidos por los operarios Ej: SMLV	S3	Luego de haber definido SMLV para el año, se verifico si se puede modificar	Se comprueba que este dato se puede modificar por parte de usuarios no autorizados
61	Comprobar si existen archivos que permitan existencia de datos duplicados	S3	Revisar la aplicación y evidenciar que permite datos duplicados	Si lo permite, se definió SMLV para 2004 con diferentes valores y lo acepto, también en una ocasión un empleado recibió doble consignación porque aparecía con dos registros de sus datos
62	Evaluar correlación de campos	S3	Se genera un nuevo registro y se estudian algunos campos que dependen de otros.	No existe relación lógica entre capos algunos campos que validan otros no se comportan así.
63 70	Evaluar documentación en las aplicaciones	S3	Revisar una aplicación y evaluar las ayudas visuales que presentan	La descripción de los campos es muy clara debido a la facilidad que presenta Data Ease para definir formas
		S5	Revisar la documentación y evaluar su calidad	La documentación es funcional ya que aporta a los usuarios conocedores del sistema apoyo en la utilización del software, pero para un nuevo usuario no es muy descriptiva
64	Valorar que tan perjudicial es la perdida del fluido eléctrico durante la ejecución de procesos complejos	S1	Entrevistar al personal usuario sobre los riesgos de perdida de información por interrupción del fluido eléctrico	En una ocasión manifiesta la auxiliar de contabilidad que perdió la información digitada de un periodo de nomina durante su actualización por interrupción eléctrica.
67	Evaluar continuidad del servicio informático en caso de errores fatales	S2	Se observa y analiza el entorno informático	Se observa que hay fallas en la UPS lo que provoca que se apague el servidor y halla perdida de tiempo, no existen equipos de respaldo.

4.3 ETAPA DE DISEÑO DE CONTROLES Y DESCRIPCIÓN DE RECOMENDACIONES

Esta etapa constituye la finalización del presente trabajo de auditoría, aquí se identifican los controles necesarios para dotar la empresa de practicas adecuadas de control de su entorno informático igualmente se hace una descripción de la forma como se puede estructurar cada uno de los controles es decir, su correspondiente recomendación.

Para el mejor entendimiento de cada uno de los controles identificados se utilizan tablas que detallan en sus columnas la siguiente información: en la primera columna hace referencia al número consecutivo que identifica al control, la segunda columna el nombre del control que a su vez constituye en una primera descripción de su recomendación, la tercera columna identifica los riesgos que son cubiertos al implementar el control correspondiente, la cuarta columna reconoce el tipo de control que puede ser General (G), Directo (R), Preventivo (P), Detectivo (D) y Correctivo (C), las columnas 5 y 6 identifica los encargados de implementar el control respectivo.

4.3.1 Diseño de controles en materia de control interno informático

Tabla 4.19 Diseño de controles en materia de control interno informático

Número del Control	Nombre del Control	Riesgos Cubiertos	Características y Responsables		
			Tipo de control	Empresa	Auditor
1	Creación de un comité de informática responsable de las principales decisiones estratégicas	1	G	√	
2	Definir un plan de informática	2	G	√	
3	Definir un administrador del entorno informático	3	G	√	
4	Definir una bitácora que registre la manifestación de incidentes en el entorno informático	4,71	GD	√	√
5	Definir buenas practicas de mantenimiento de software y separar las funciones de desarrollo y explotación	5,72,73	RP	√	√
6	Hacer un estudio que evidencia o no la necesidad de iniciar un nuevo proyecto de sistematización	6	G	√	√
7	Definir un procedimiento técnico para adquirir soluciones informáticas	7	GP	√	√
8	Estudiar y definir una metodología de desarrollo de aplicaciones incluido un estudio previo de viabilidad	8	GP	√	√
9	Definir un estudio previo de oportunidad y necesidad en la adquisición de soluciones informáticas	9	G	√	√
10	Definir buenas prácticas para nombrar archivos	10	RP	√	√
11	Definir un procedimiento de puesta en marcha de nuevas aplicaciones	11	GP	√	√
12	Definir un encargado de hacer seguimiento y hacer cumplir los servicios de tecnologías contratados por la empresa	12,20	GP	√	
13	Definir políticas de calidad que gobiernen la función informática	13	G	√	√
14	Actualizar o complementar la documentación de manuales de usuario y aplicaciones	14,70	DP	√	√
15	Diseñar un procedimiento adecuado de mantenimiento de aplicaciones	15	RP	√	√
16	Crear biblioteca de programas fuentes	16,74	GP	√	√
17	Indicar criterios de validación de datos	17	RP	√	√

Número del Control	Nombre del Control	Riesgos Cubiertos	Características y Responsables		
			Tipo de control	Empresa	Auditor
18	Crear un centro de computo alterno que garantice la continuidad del servicio	18	RP	√	√
19	Definir y divulgar un modelo de seguridad de la información y seguimiento a usuarios	19	GP	√	√
20	Definir y divulgar una cultura de correcta utilización del recurso informático	21	GP	√	√
21	Creación de Biblioteca de programas, centro de mantenimiento y documentación	22	RC	√	√
22	Definir un procedimiento adecuado de copias de seguridad del conjunto datos y aplicaciones	23,24	RC	√	√
23	Plan de contingencias	25,26,37	RC	√	√
24	Restringir acceso al cuarto del servidor	27,75	RP	√	√
25	Evaluar controles sobre incendios, inundaciones interrupciones eléctricas e intrusos	28,36	GD		√
26	Definir funciones del Administrador de la base de datos	31,32	GP	√	√
27	Diseñar un modelo de seguridad que administre información y tecnologías	33,34,42	DP	√	√
28	Creación de un manual de configuración del entorno informático	35,43,77,79	G		√
29	Definir un encargado de seguridad y divulgar una cultura de responsabilidad en el uso adecuado de TI.	38	DP	√	√
30	Definición de un procedimiento de asistencia técnica y mantenimiento a los recursos de TI.	39,41	GP	√	√
31	Definir un procedimiento que garantice de manera razonable la entrada, actualización, validación y el mantenimiento completo y exacto de los datos	44,46,47,48,49,66	GP	√	√

32	Definir información que debe ser revisada antes de ser ingresados al sistema	45	DP	√	
33	Definir un criterio de almacenamiento de información Histórica y Actual	50	DP	√	
34	Rediseñar los controles sobre salida de datos Balanceo y Conciliación	51	GD	√	
35	Creación de perfiles de usuario	53	DP	√	√
36	Definición de pistas de auditoria	54	GD	√	√
37	Diseño de módulos de acceso al SI., basado en perfiles de usuario	55	DP	√	
38	Nombrar un encargado de actualización y ejecución de corridas programadas y no programadas	56,69	DP	√	
39	Asegurar que el SI., valide en sus campos el tipo de dato adecuado según el formato	57	DP	√	√
40	Rediseñar algunas formas definiendo campos necesarios y no necesarios	58	DP	√	√
41	Definir limites en los campos	59	DP	√	√
42	Asegurar funcionalidad de la correlación de campos	60,62	DP	√	√
43	Eliminar redundancia	61	DP	√	√
44	Implementar ayudas desplegables en el SI, sobre campos claves	63	GP	√	
45	Estructurar un Departamento de Informática	68	G	√	
46	Definir una política para la asignación, uso y cambio de contraseñas	76	DP	√	√
47	Programa de capacitación del personal en el manejo de recursos de TI.	80	GP	√	√
48	Diseñar un esquema de seguridad que administre la Red de Sevicol	81	DP	√	√
49	Divulgar un modelo de copias de seguridad de información vital por puestos de trabajo	82	DP		√
50	Considerar un modelo de investigación en TI., para ser aprovechadas o tenidas en cuanta por la empresa.	83	G	√	√

4.3.2 Descripción de recomendaciones

En esta sección, se hace la descripción de las recomendaciones de cada uno de los controles identificados en el apartado anterior.

No. 1 Creación de un comité de informática responsable de las principales decisiones estratégicas así:

1. Este comité puede ser conformado por un representante de la alta dirección (Gerente o Subgerente), los ingenieros responsables de informática de la compañía y la directora administrativa.

2. Sus funciones principales son hacer seguimiento al funcionamiento del entorno informático, definir la dirección tecnológica de la empresa, considerar oportunidades que puede brindar la implantación de nuevas tecnologías en el mejor funcionamiento de la organización, definir prioridades a corto plazo, elaboración y/o aprobación del plan de informática

3. Definir periodicidad de reunión del comité.

No. 2 Definir un plan de informática: El plan de informática determina los objetivos en tecnología de la empresa, define los plazos y el procedimiento a seguir para conseguir las metas planteadas.

No. 3 Definir un administrador del entorno informático: Esta persona será la responsable de mantener en funcionamiento optimo el recurso informático de la empresa, igualmente es la persona a la cual pueden acudir los usuarios en caso de incidentes o capacitación, además conformara el comité de informática, velara por el cumplimiento de sus decisiones y hará seguimiento de los diferentes proyectos o contratos a nivel de tecnología que estén vigentes.

No. 4 Definir una bitácora que registre la manifestación de incidentes en el entorno informático: en este libro se consignara los incidentes y manifestaciones que los usuarios hagan acerca del funcionamiento del entorno informático. Aquí se anotará en forma clara y detallada el acontecimiento presentado con fecha y nombre del que la realiza. El objetivo de esta práctica es llevar estadísticas de incidentes e ir descubriendo anomalías deL funcionamiento del servicio informático para su posterior mantenimiento.

No. 5 Definir buenas prácticas de mantenimiento de software y separar las funciones de desarrollo y explotación: Este control restringe el acceso a los usuarios de opciones propias del administrador como cambio de contraseñas, acceso al código fuente. También contribuye con buenas prácticas de mantenimiento donde estas no

sean efectuadas sobre aplicaciones en funcionamiento y se tengan en cuenta los incidentes y observaciones registrados en la bitácora. Es decir, definir perfiles de usuario y aunque en SEVICOL LTDA, la función de desarrollo y explotación se ejecuta por la misma persona recomienda realizar el mantenimiento en un ambiente de desarrollo y luego pasarlo a explotación.

No. 7 Definir un procedimiento técnico para adquirir soluciones informáticas: Este procedimiento define algunos aspectos a tener en cuenta cuando se adquieren soluciones tecnológicas así:

- **Redactar un pliego de condiciones que incluya**
- Descripción de las funciones a procesar
- Volúmenes a procesar
- Plazos para la puesta en marcha
- Obligaciones en materia de seguridad
- Los datos que deben ser controlados por los archivos
- Definir prioridades de funciones iniciales

- **Estudiar y comparar varias propuestas antes de la elección definitiva**
- **Apoyar la elección final a partir de:**
- La calidad de las propuestas recibidas
- Visitas a otras compañías que tienen el mismo programa

- Consideraciones sobre el proveedor como: envergadura, participación en el mercado, calidad de los asesores, perennidad de firma
- Calidad de la documentación

Prever en el contrato firmado con el Proveedor :

- Compromiso por el procesamiento de las aplicaciones definidos en el pliego de condiciones
- Compromiso de procesamiento de los volúmenes de información también definidos
- Cláusulas por incumplimiento
- Definición precisa de las asistencia prestada como: capacitación, documentación, asistencia en la puesta en marcha, mantenimiento inicial
- Condiciones de mantenimiento del programa
- Condiciones para el pago
- La empresa disponga de los programas fuentes: este punto especialmente se debe analizar dependiendo de la envergadura de la empresa que vende el servicio, si la compañía necesita hacerle modificaciones al software.

No. 8 Estudiar y definir una metodología de desarrollo de aplicaciones incluido un estudio previo de viabilidad: Definir un método único y apropiado de desarrollo de aplicaciones es una tarea difícil, ya que una precisión teórica no garantiza nada y seria

mejor definir esta metodología a partir de los resultados que se esperan. Entre los métodos de desarrollo mas difundidos están:

- **Ciclo de vida clásico de desarrollo de sistemas:** incluye las actividades de investigación preliminar, determinación de requerimientos del sistema, diseño del sistema, desarrollo de software, prueba de sistemas e implantación. Entre algunas de las características de este procedimiento podemos mencionar que involucra varios departamentos generalmente toda la organización, su tiempo de desarrollo es largo, procesa grandes volúmenes de información y es cómodo para ser manejado por varios equipos del proyecto.

- **Método de desarrollo por análisis estructurado:** este método es ideal cuando se inician proyectos grandes y complejos y no se puede abarcar de manera completa, sugiere la división del sistema en componentes y la construcción de un modelo del sistema. Utiliza símbolos gráficos para describir movimiento y procesamiento de datos incluye diagramas de flujo y diccionario de datos.

- **Método del prototipo de sistemas:** desarrollo iterativo en continua evolución el usuario participa directamente en el proceso. Es útil para probar la factibilidad del sistema, determinar requerimientos de los usuarios, apropiado

cuando el desarrollador tiene poca experiencia o información o donde los costos y riesgo de errores son altos.

- **Proceso unificado de desarrollo:** combina todas las características de los métodos anteriores pero su utilidad se muestra cuando el desarrollo es orientado a objetos.

  -Dirigido por casos de uso: se centra en la funcionalidad que el sistema debe poseer para satisfacer las necesidades de un usuario.

  -Centrado en la arquitectura: concepto similar a la arquitectura de un edificio, varios planos con diferentes aspectos del edificio, tener una imagen completa del edificio antes de empezar a construir.

  -Arquitectura en software: diferentes vistas del sistema (Estructural, funcional, dinámico), la arquitectura determina la forma del sistema, casos de uso determinan la función del sistema.

  -Iterativo e incremental: detección temprana de riesgos, administración adecuada del cambio, mayor grado de reutilización, mayor experiencia para el equipo de desarrollo.

La recomendación sugiere utilizar un procedimiento de desarrollo ampliamente difundido y concentrar la selección a partir de la factibilidad de ejecutar el proyecto a partir de:

- **Factibilidad técnica:** el trabajo para el proyecto ¿puede realizarse con el equipo actual, la tecnología existente de software y el personal disponible? Si se necesita nueva tecnología ¿Cuál es la posibilidad de desarrollarla?
- **Factibilidad económica:** al crear el sistema ¿Los beneficios que se obtienen serán suficientes para aceptar los costos?, ¿Los costos asociados con la decisión de no crear el sistema son tan grandes que se debe aceptar el proyecto?
- **Factibilidad operacional:** Si se desarrolla e implanta, ¿Será utilizado el sistema?, ¿Existirá cierta resistencia al cambio por parte de los usuarios que dé como resultado una disminución de los posibles benéficos de la aplicación?

No. 9 Definir un estudio previo de oportunidad y necesidad en la adquisición de soluciones informáticas: el comité de informática será encargado de dar cumplimiento a esta recomendación. A partir del crecimiento corporativo y aparición de recursos de tecnologías de la información que faciliten la realización de las tareas en la empresa. Este control se orienta a determinar áreas de oportunidad que puede brindar la función informática en los siguientes aspectos:

- Apoyo a la alta dirección (Sistemas de información estratégico)
- Apoyo a las agencias (Sistemas de información integrales)
- Participación de informática en proyectos claves de la compañía
- Actualización tecnológica

- Capacitación o actualización profesional del personal de informática
- Creación y difusión de nuevos servicios de informática para el negocio

No. 10 Definir buenas prácticas para nombrar archivos

No. 11 Definir un procedimiento de puesta en marcha de nuevas aplicaciones: entre las características mas importantes de este procedimiento se puede mencionar.

- La formación de los usuarios: capacitación y formación en el uso del nuevo sistema.
- Documentación de la aplicación: teniendo en cuenta la documentación de desarrollo y de usuarios.
- Recuperación de archivos: se refiere a la migración de los datos
- El impacto del nuevo sistema en la organización y en los procedimientos administrativos
- Implantación física de los equipos
- Validación del software
- Seguridad: recuperación en caso de incidentes, aspectos de control como segregación de funciones, control jerárquico, autorizaciones para acceder el sistema

No. 12 Definir un encargado de hacer seguimiento y hacer cumplir los servicios de tecnologías contratados por la empresa

No. 13 Definir políticas de calidad que gobiernen la función informática: una política de calidad que garantice en términos razonables una administración eficaz y eficiente el entorno informático en SEVICOL LTDA., es el cumplimiento de los controles, procedimientos y recomendaciones del manual de control interno informático definido para la compañía.

No. 14 Actualizar o complementar la documentación de manuales de usuario y aplicaciones: esta recomendación sugiere que la empresa tenga en su documentación aspectos tales como:

- La documentación de desarrollo y explotación:
  - Descripción del contenido de los archivos
  - Descripción de los procesos
  - Descripción de los programas
  - Historial de las operaciones de mantenimiento.
  - Instrucciones para su utilización
  - Descripción de los controles para la explotación a ser llevados a cabo en el momento de ejecutar cada proceso

- La documentación para usuarios debe contener:
  - Descripción general de las aplicaciones
  - Descripción de las transacciones
  - Descripción de los listados editados
  - Explicación de los mensajes de anomalías.

No. 15 Diseñar un procedimiento adecuado de mantenimiento de aplicaciones: A razón que en SEVICOL LTDA., las modificaciones y mantenimiento de aplicaciones se hacen a partir de necesidades de los usuarios, nuevas leyes y regulaciones y no seguido de un proceso formal de mantenimiento. Es decir, no hay un equipo de estudio (Desarrollador) permanente. Se recomienda formalizar por escrito estas peticiones y modificaciones por el solicitante y a su vez, el responsable de implementar y dar mantenimiento a las aplicaciones formalizar también por escrito su actuación y luego archivar estas novedades en la documentación respectiva de programas que nos permitirá llevar un control de crecimiento adecuado.

No. 16 Crear biblioteca de programas fuentes: esta recomendación sugiere crear un depósito donde se almacene el código fuente de las aplicaciones para que sean usados cuando se necesite. También se recomienda actualizarlas debido a que las modificaciones se hacen sobre las aplicaciones en funcionamiento lo que puede hacer incompatibles los fuentes almacenados con el código objeto actualmente en ejecución.

No. 17 Indicar criterios de validación de datos: aquí se recomienda cumplir con unos principios básicos de toma de datos así:

- Revisión y aprobación de los documentos fuentes por personal autorizado antes de ser ingresados al sistema
- Control por totalización de los lotes de introducción, que comprueba que todo documento hay sido introducido una única vez y correctamente.
- Controles de compatibilidad
- Visualización para validación desde la introducción desde el texto correspondiente

En general los procedimientos de registro de datos debe cumplir con principios de exhaustividad (que todo dato que debe ser introducido lo sea de verdad), realidad (que no sean introducidos datos que no deban ser), exactitud (que los datos no tengan errores).

No. 18 Crear un centro de computo alterno que garantice la continuidad del servicio: aunque un centro de computo alterno implicaría aumento de costos se recomienda identificar un sitio alterno donde se tengan copias de aplicaciones y datos, documentos de puesta en marcha y reinicio de operaciones y configuración de equipos. Esta recomendación se detalla más en el plan de contingencias.

No. 19 Definir y divulgar un modelo de seguridad de la información y seguimiento a usuarios: reconociendo que la información constituye un activo valioso para la empresa se recomienda implantar un modelo de seguridad de la información que cubra aspectos tales como:

- Identificación única de usuarios, control de acceso
- Asignación de estaciones de trabajo
- Definición de responsabilidades sobre los procesos y transacciones administrativas
- Definir perfiles de uso de archivos y bases de datos
- Definir información clasificada
- Generar y difundir una cultura de riesgo informático

No. 20 Definir y divulgar una cultura de correcta utilización del recurso informático: El recurso informático es hoy en día una herramienta muy preciada en todos los ámbitos ya que hace más fácil muchas de nuestras labores, por lo que se recomienda generar y divulgar una cultura que aprecie y utilice correctamente este recurso orientado a:

- Cuidados y mantenimiento del computador
- Uso de Internet y de antivirus
- Piratería de software

- Copias de seguridad
- Capacitación

No. 21 Creación de Biblioteca de programas, centro de mantenimiento y documentación: este control permite organizar en un solo sitio y conocido por los demás usuarios una biblioteca de programas fuentes, aplicaciones de oficina, antivirus y otros programas, como también documentación de aplicaciones, manuales de usuario y los elementos de mantenimiento y reparación (repuestos) todo lo anterior con el objetivo de saber donde buscar en caso que el ingeniero responsable no se encuentre.

No. 22 Definir un procedimiento adecuado de copias de seguridad del conjunto datos y aplicaciones: estas copias se realizaran cada Lunes y en caso de festivo el Martes, se mantendrá una copia en el disco duro del computador asignado al gerente administrativo y dos copias en disco extraíble una de las cuales se intercambiara con la que se encuentre en el sitio de respaldo. El responsable de ejecutar este procedimiento es el Ing. Carlos Arturo Rueda.

No. 23 Plan de contingencias: este mecanismo de control permitirá de forma razonable reiniciar operaciones en caso de emergencias totales o parciales de la función informática. Se recomienda que este plan contenga aspectos tales como:

- Análisis: estudio del ambiente físico y organizacional de la compañía, incluido un análisis de riesgos.
- Definición: determinar emergencias susceptibles por la compañía y procedimientos de reacción, también definición del plan de respaldo donde se incluyen los elementos necesarios para el reinicio de operaciones.
- Implantación: capacitación, entrenamiento y pruebas
- Mantenimiento: actualización del plan a partir de nuevas normas de seguridad.

No. 24 Restringir acceso al cuarto del servidor: Debido a la importancia que representa el servidor dentro del funcionamiento del entorno informático y además, porque en el mismo sitio funciona Monitoreo (servicio de vigilancia) se recomienda restringir y controlar el ingreso a este sitio mediante señales de advertencia, definición de personas con permiso de ingreso y registro de personas que hayan sido autorizadas igualmente se sugiere que la puerta permanezca cerrada.

No. 25 Evaluar controles sobre incendios, inundaciones interrupciones eléctricas e intrusos: este control se evaluara en la fase de análisis del plan de contingencias, específicamente en la evaluación del ambiente existente.

No. 26 Definir funciones del Administrador de la base de datos: algunas de estas funciones son:

- Optimizar la Base de Datos: normalizar la BD, eliminar redundancia, mantener integridad funcional de los datos
- Gestión de los Datos: permitir la realización de diferentes procesos de cálculo y edición a partir de los datos registrados, facilitar consultas y generar informes.

No. 27 Creación de un manual de configuración del entorno informático: este manual permitirá identificar los elementos, productos y herramientas que constituyen el entorno informático de SEVICOL LTDA. Con el fin de conocerlo mejor, aprovecharlo y poder controlarlo.

No. 28 Definir un encargado de seguridad y divulgar una cultura de responsabilidad en el uso adecuado de TI: esta responsabilidad se le asigna al Gerente Administrativo

No. 29 Definición de un de procedimiento de asistencia técnica y mantenimiento a los recursos TI: esta recomendación sugiere definir algunos criterios a tener en cuenta cuando se contrate el servicio de mantenimiento del recurso informático.

- Proveedor del servicio (que sea reconocido)
- Definir términos del contrato: duración, costo, lo que cubre, mano de obra, repuestos, renegociación.
- Servicios que ofrece

- Tiempo de respuesta y horario de atención

No. 30 Definir información que debe ser revisada antes de ser ingresados al sistema: el objetivo de este control es verificar, validar y supervisar la información antes de ser procesado por el SI., este control es de carácter preventivo tipo advertencia con el fin de recordar a los digitadores que su trabajo será objeto de supervisión y así serán estimulados a ejecutarlo con mayor atención.

No. 31 Definir un criterio almacenamiento de información Histórica y Actual: debido a los grandes volúmenes de información que maneja la empresa se recomienda determinar que datos son históricos y que no son procesados y cuales si, esto con el fin de liberar espacio en disco y hacer más rápido los tiempos de procesamiento.

No. 32 Rediseñar los controles sobre salida de datos Balanceo y Conciliación: la forma como se lleva este control del tipo control de comparación es adecuado y cumple con sus objetivos que es verificar y encontrar inconsistencias en cuentas y transacciones. Se recomienda llevar un registro de incidentes en la bitácora con el fin de identificar responsabilidades a nivel de usuario o procesos automatizados y tomar acciones correctivas que disminuyan la probabilidad de ocurrencia de estos eventos.

No. 33 Definición de pistas de auditoria: en muchas organizaciones es frecuente encontrar una confianza excesiva en los SI., y por otra parte en frecuente encontrar

que los usuarios imputan la mayoría de errores al mal funcionamiento de los SI., y no aceptan su responsabilidad. Esta recomendación busca controlar esta situación llevando en la medida de lo posible las aplicaciones de SEVICOL LTDA., a un estado de confiabilidad, seguridad y disponibilidad aceptable implementando procedimientos de auditoria y control entre las que podemos mencionar:

- Rastrear una transacción por cada paso del proceso y tener la capacidad de examinar los valores de datos intermedios producidos durante el procesamiento.
- Imprimir registros y transacciones seleccionados del sistema que cumplan ciertos criterios (tales como una cuenta altamente activa o una cuenta con saldo alto) para validar la precisión y autenticidad tanto de las transacciones como de los resultados.
- Mantener un balance constante en el sistema cuando éste implique cuestiones financieras y reportar si el sistema está balanceado
- Producir un diario detallado de todas las transacciones y el efecto de éstas en los saldos de las cuentas o en los registros del archivo maestro.
- Proporcionar los controles suficientes en la entrada, tales como controles y cuenta de los lotes y transacciones
- Controles de acceso a las aplicaciones
- Perfiles de usuarios.

No. 34 Nombrar un encargado de actualización y ejecución de corridas programadas y no programadas: esta persona será la encargada de ejecutar los procesos de actualización del archivo maestro su objetivo es prevenir perdida de información, y validar que los datos sean exactos y completos.

No. 35 Asegurar que el SI., valide en sus campos el tipo de dato adecuado según el formato: es decir, que campos numéricos no acepten caracteres alfabéticos

No. 36 Rediseñar algunas formas definiendo campos necesarios y no necesarios: esto hace parte del mantenimiento de la base de datos

No. 37 Definir límites en los campos: esta recomendación surge debido a que algunos campos numéricos aceptan cifras que no corresponden a la realidad de la empresa, por ejemplo el campo de sueldo a pagar.

No. 38 Asegurar funcionalidad de la correlación de campos: esta característica de una base de datos permite validar información y se ha detectado que algunos campos que dependen de otros no funcionan así.

No. 39 Eliminar redundancia: esta recomendación hace parte del mantenimiento de la base de datos.

No. 40 Implementar ayudas desplegables en el SI, sobre campos claves: estos mensajes y comentarios pretender informar sobre el funcionamiento de algunos procesos y su carácter es de tipo preventivo.

No. 41 Estructurar un Departamento de Informática: esta característica constituye una buena práctica de control interno y su objetivo es centralizar y organizar toda la responsabilidad de esta función a este órgano.

No. 42 Definir una política para la asignación, uso y cambio de contraseñas: la protección y confidencialidad de los datos constituye un objetivo clave de la función de seguridad. Una medida para lograr este supuesto es través de la asignación de contraseñas de acceso que restringe el ingreso a las aplicaciones y nos permite identificar los usuarios. Algunas características para asignar contraseñas son:

- Definir contraseñas de acceso a la red y a las aplicaciones
- De carácter individual
- Difíciles de descifrar
- Administradas por el Director Administrativo y responsable de sistemas.

No. 43 Programa de capacitación del personal en el manejo de recursos de TI.

No. 44 Diseñar un esquema de Gestión que administre la Red de SEVICOL: esta recomendación sugiere un mejor aprovechamiento de este servicio de comunicaciones interna, igualmente se debe estructurar esta función y controlar sus servicios. Este procedimiento de gestión involucraría aspectos tales como:

- Documentación de los detalles de red, esquema de la red, descripción de la configuración de hardware de comunicaciones, descripción del software que se utiliza, control de la red y consideraciones relativas a la seguridad de la red, flujos de información, número de puestos de trabajo, número de personas por puesto de trabajo, niveles de control y demás elementos relacionados.
- Administrador de la red: persona encargada de crear puestos de trabajo, asignación de usuarios, validación de usuarios, definir normas de seguridad para conexión con el exterior, registro y solución de incidentes.
- Seguridad de la red física y lógica.

No. 45 Divulgar un modelo de copias de seguridad de información vital por puestos de trabajo:

No. 46 Considerar un modelo de investigación en TI, para ser aprovechadas o tenidas en cuanta por la empresa: se recomienda orientar esta investigación hacia las áreas de oportunidad que puede brindar las TI, identificadas anteriormente para la

empresa y se defina también una periodicidad para discutir estos temas y su viabilidad.

CONCLUSIONES

- Se recomienda incentivar la Practica Empresarial como modalidad de trabajo de grado, por el aporte y experiencia que le ofrece a los futuros profesionales. Además porque contribuye a dar soluciones directas a las necesidades del sector empresarial y de paso cumplimos con nuestra misión institucional.

- La Auditoría Informática es una disciplina mal entendida y tal vez por esto es porca la difusión que hay en nuestra comunidad académica, con este trabajo se muestra que es una herramienta eficaz y se presenta como una alternativa muy viable de oportunidad de negocio la cual debemos tener en cuenta.

- Las organizaciones empresariales viven inmersas en un laberinto de funciones y actividades que son apoyadas por soluciones informáticas, pero estas a veces contribuyen agrandandado un poco el problema por la falta de un control administrativo sobre esta función.

- Es importante reconocer que el recurso informático es solo una herramienta de apoyo a las actividades administrativas y operativas de la empresa y su éxito se

basa a partir de una clara comprensión de las funciones de la organización y de una acertada definición de sus necesidades.

- El tener claro lo que se quiere y el reconocimiento de nuestras fortalezas son el principio para la consecución de nuestras metas. La mediocridad no existe solo existen personas mal ubicadas.

BIBLIOGRAFÍA

HERNANDEZ HERNANDEZ, Enrique. Auditoría Informática: Un enfoque metodológico y práctico, Compañía Editorial Continental, 2da Edición, México, 2000.

YANN, Derrien. Técnicas de la auditoría informática, Ediciones Alfaomega S.A., México 1995.

PIATTINI, Mario G y DEL PESO, Emilio. Auditoría Informática: Un enfoque práctico, Editorial Alfaomega, 1ra Edición, Bogotá, 1998.

PINILLA, José Dagoberto. Auditoría Informática: Aplicaciones en Producción, Editorial ecoe, 1ra Edición, Bogotá, 1997

www.isaca.org Asociación de Auditoría y Control en Sistemas de Información.

GOMEZ F., Luis Carlos. Introducción a la Auditoría de Sistemas, Ediciones UIS, Bucaramanga, 1993

ECHENIQUE GARCÍA, José Antonio. Auditoría en Informática. Segunda edición. México: McGraw-Hill.

DataEase International, Tomo 1. Guía del Usuario, Tomo 2 Administración de la Base de Datos/Guía para el desarrollo de Aplicaciones, Tomo 3. Guía de Lenguaje de Consulta de DataEase (DQL).

SENN, James A. Análisis y diseño de sistemas de información. Segunda Edición. México: McGraw-Hill Interamericana. de México

FERRANDO GIRON, Santiago. GARCIA TOMAS, Jesús. PIATTINI VELTHIUS, Mario, Redes para Proceso Distribuido: Área Local, Arquitecturas, Banda Ancha, Editorial Alfaomega, 1ra Edición, Bogotá, 1997.

STAMPER, David A, Local Area Networks, Austin U.S.A. Editorial Prentice Hall 2000

GOMEZ F., Luis Carlos, Planeación de Proyectos – Un enfoque para Ingeniería de Sistemas e Informática, Bucaramanga, 2001.

GRECH M. Pablo, Introducción a la ingeniería -Un enfoque a través del diseño, 1ra Edición, Bogotá, D.C. Editorial Prentice Hall, 2001

ANEXO A

PLAN DE CONTINGENCIAS

(SEVICOL LTDA.)

A.1 Presentación

Dentro de un marco de control interno aceptado el plan de contingencias constituye un elemento esencial, reconociendo que el objetivo principal de una organización en sus áreas funcionales es la operatividad es decir, la continuidad de las operaciones ante desastres, sabotajes o mal funcionamiento de equipos; el plan de contingencias se presenta como una herramienta vital que garantizara en términos razonables la continuidad de las operaciones.

Tabla B.1 Desastres informáticos

Desastres Informáticos	
Desastres Naturales	Inundaciones, terremotos
Desastres locales	Incendios, sabotajes, interrupciones eléctricas
Fallas en los equipos	Servidor central, unidades de almacenamiento (disco duro), CPU, Mother board
Errores de software	SO, virus, errores en los programas
Errores humanos	Perdida de personal clave, errores de usuario

A.2 Ciclo de desarrollo del plan de contingencias

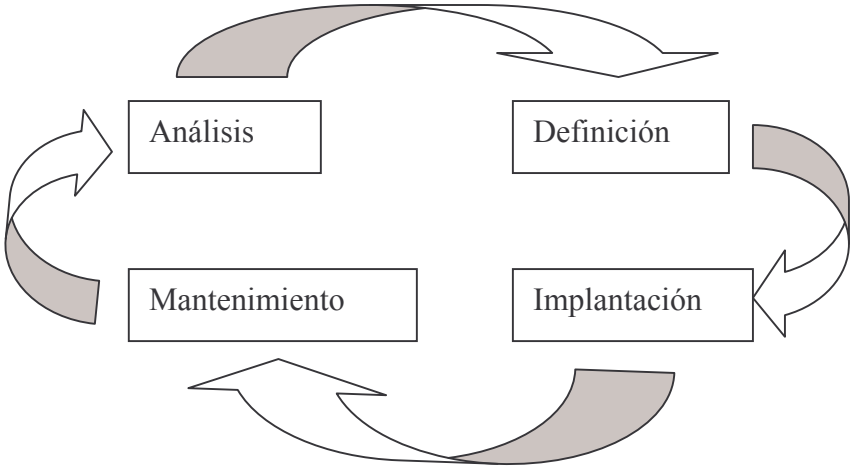


Figura B.1 Fases del ciclo del plan de contingencias

Fases	Actividades
Análisis	Evaluación del ambiente Identificación de elementos críticos Inventario de elementos a preservar, salvar y recuperar Análisis especifico de amenazas Análisis de riesgos
Definición	Reacción a emergencias Desarrollo del plan de reacción Procedimientos del plan de reacción Responsabilidades Plan de respaldo Almacenamiento y depósitos Recursos de procesamiento Procedimientos de acción Controles de acción de recuperación
Implantación	Documentación Preparación Pruebas
Mantenimiento	Monitoreo del ambiente Causas del cambio Reevaluaciones periódicas

A.2.1 Fase de Análisis

El objetivo de esta fase es lograr el conocimiento del entorno informático, identificar el grado de exposición de los recursos y determinar la prioridad en la protección de algunos recursos dentro del plan de contingencias.

A.2.1.1 Evaluación del ambiente existente

Esta fase nos permite conocer el ambiente informático de la empresa es decir, sus recursos, la forma como interactúan sus elementos, las ventajas, beneficios y fallas que presentan, el ambiente organizacional entre otras. Los aspectos a evaluar se presentan en la siguiente tabla.

Tabla B.2 Aspectos a evaluar

Aspectos a Evaluar	Elementos por cada aspecto
Lugar físico	Fuente eléctrica, espacio, ubicación
Controles físicos	Controles de seguridad y acceso, agua, temperatura
Ambiente del personal	Hostilidad de personal, actitudes y aceptación de controles
Ambiente político, legal y civil	Terrorismo, sabotaje
Configuración	Configuración del entorno informático de la empresa

A.2.1.2 Identificación de elementos críticos

En este punto es importante determinar cuales son los elementos esenciales para una nueva puesta en marcha del entorno informático en lo referente a las aplicaciones, personal, configuración y datos

A.2.1.3 Inventario de elementos a preservar, salvar y/o recuperar

- Datos (almacenamiento y respaldo críticos)
- Programas (de aplicación o soporte)
- Equipos
- Documentación
- Suministros, material y medios
- Personal

A.2.1.4 Análisis especifico de amenazas

Aquí se debe prestar especial atención a las amenazas derivadas de la naturaleza del servicio que presta SEVICOL LTDA. además de las que se presentan a continuación.

Tabla B.3 Amenazas especificas

Incendio	Elementos afectados
Interrupciones del hombre	Sabotaje, violaciones de seguridad
Desastres naturales	Inundación, terremoto
Fallas de energía	Corte de líneas, fallas eléctricas

A.2.1.5 Análisis de riesgos

Permite valorar el impacto que algunas amenazar pueden tener sobre los elementos del entorno informático. Además dado que es un estudio lo suficientemente profundo puede proporcionar razones valederas para implementar acciones de control lo antes posible.

A.2.2 Definición del plan de contingencias

Esta fase es la estructuración propiamente dicha del plan de contingencias debe incluir: reacción a emergencias, plan de respaldo y plan de acción de recuperación.

A.2.2.1 Reacción a emergencias

Es la forma como se atenderá una eventual emergencia, se debe definir la secuencia de desarrollo de reacción, las acciones a ejecutar y los responsables. Dentro del plan de reacción se deben incluir aspectos tales como:

- Definición y reconocimiento de un caso de emergencia
- Descripción de pasos específicos bajo declaración de emergencia
- Secuencia de procedimientos durante estado de emergencia
- Lista de personal responsable
- Lista de contactos (Proveedores, autoridades, asistencia técnica)

A.2.2.2 Plan de respaldo

Este plan sugiere los elementos necesarios para reiniciar las actividades además, como punto clave es la identificación de un sito alterno donde se almacenaran los elementos mencionados y se continuaran las operaciones.

- Ubicación del centro de computo alterno
- Programas de: soporte y aplicación
- Suministros: papel, formas preimpresas, lista de proveedores, datos
- Documentación

A.2.2.3 Plan de acción de recuperación

Este desarrollo es similar al plan de acción de emergencias.

A.2.3 Implantación del plan de contingencias

El siguiente paso luego de haber analizado y definido el plan de contingencias es su implantación es decir, la incorporación de los procedimientos determinados dentro del ámbito organizacional. Incluye aspectos tales como: Documentación que es la información necesaria que me permite conocer el entorno informático, entrenamiento dirigido al personal responsable de responder y respaldar las acciones del plan de contingencias como forma de estar preparados ante eventos indeseables y pruebas que me permitan evaluar la eficacia del plan.

A.2.4 Mantenimiento del plan de contingencias

Debido a la naturaleza dinámica de las organizaciones es decir, a los cambios que se presentan (rotación de personal, reemplazo y cambio de tecnologías) se requiere de un mantenimiento del plan de contingencias que actualicé los recursos a proteger y determine nuevas prioridades.

A.2.4.1 Monitoreo del ambiente

El monitoreo del ambiente que en esencia es una actividad de observación sobre eventos en otras organizaciones o actualización a partir de nuevas recomendaciones

sobre emergencias, permite identificar nuevos riesgos o su desaparición y se constituye como elemento clave para un plan de contingencias eficaz.

A.2.4.2 Causas del cambio

Las causas que pueden dar origen a un cambio en el plan de contingencias en nuestro caso referente al entorno informático son:

- Equipos
- Medio de telecomunicaciones
- Programas de soporte y aplicaciones
- Estructura organizacional
- Ambiente físico

PLAN DE CONTINGENCIAS
(DESARROLLO)

1. Análisis

1.1 Planta física

SEVICOL LTDA, esta ubicada en la carrera 37 No.42-73, barrio San Pío de la ciudad de Bucaramanga, la instalación locativa consta de una edificación de tres pisos donde funciona el área administrativa cuya construcción se realizó en cemento y ladrillo, pisos en cemento y cerámica y paredes estucadas y pintadas, cuenta con todas las especificaciones de iluminación natural y artificial, proporcionada por luminarias fluorescentes e incandescentes respectivamente, la ventilación es proporcionada por puertas, ventanas y aire acondicionado.

1.2 Controles físicos

SEVICOL LTDA, cuenta con los respectivos controles detectivos de seguridad tales como detectores de humo, censores de movimiento y cámaras. Además, en la entrada principal permanece un vigilante las 24 horas al igual que en el cuarto de monitoreo, el aspecto a tener en cuenta como posible falla de seguridad es el referente al acceso de personal al edificio, ya que este se efectúa sin ningún tipo de requisa o registro y este personal se puede desplazar fácilmente por toda la edificación.

1.3 Ambiente del personal

El ambiente laboral en la compañía a nivel administrativo se puede considerar normal, donde se manifiesta simpatía y confianza entre empleados y la mayoría son antiguos. Además, la empresa incentiva sus empleados con bonificaciones, agasajos, capacitación y reconocimiento de su labor. Igualmente como el anterior aspecto, el

riesgo se presenta en el ámbito operativo (vigilantes, escoltas) debido a la rotación y cancelación de contratos, algunos de estos por su situación económica y al encontrarse sin empleo se pueden mostrar hostiles por lo que es prudente considerar medidas de seguridad que controles incidentes originados por esta situación.

1.4 Ambiente político, legal y civil

Por la naturaleza del servicio que presta la compañía de seguridad y vigilancia, en donde su objetivo es proteger los bienes y la seguridad de sus clientes previniendo acciones delictivas, es importante tener en cuenta que la empresa puede ser objeto de acciones del hampa como terrorismo además, existen empleados insatisfechos que se pueden prestar para cometer tales eventos por lo cual conviene proteger el edificio y hacer más eficiente el control sobre el ingreso de personal al edificio.

1.5 Configuración

Este aspecto cubre lo referente a la configuración del entorno informático de la compañía donde se presentan los elementos que lo conforman tales como: inventarios, características de la red, servidor y aplicaciones, organigramas, planos de la empresa por pisos con sus dependencias y las responsabilidades de los funcionarios.

1.6 Identificación de elementos críticos

De este apartado se puede considerar también, el inventario de elementos a preservar, salvar y/o recuperar

Recurso	Descripción
Aplicaciones	Nomina, facturación, contabilidad y cartera
Datos	De respaldo, algunos contratos e información de clientes
Personal	Por su conocimiento y habilidad en cuanto al manejo del recurso tecnológico los ingenieros Juan Carlos Patiño y Carlos A. Rueda
Configuración del entorno informático	Documento que contiene una descripción detallada de los elementos que constituyen el entorno informático así como sus interacciones.
Equipos	Como elemento clave del entorno informático esta el Servidor donde se alojan aplicaciones y datos

1.6 Análisis especifico de amenazas

Las amenazas que se pueden identificar como causantes de daños o interrupción del funcionamiento normal de SEVICOL LTDA. son: Incendios, sabotajes, atentados, terremotos, fallas eléctricas, daño del servidor o ausencia al mismo tiempo de los ingenieros responsables del área informática.

1.7 Análisis de riesgos

A partir del análisis de riesgos que se desarrollo en la auditoria se seleccionaron los riesgos que hacen parte y competen en forma directa al plan de contingencias. Además, son una forma de evidenciar el grado de exposición y la necesidad de tener en cuenta prioridad para implementar acciones de control sobre los mismos.

Proceso	Número	Riesgo	Impacto							Valoración		
			Integridad	Eficiencia	Efectividad	Disponibilidad	Cumplimiento	Confidencialidad	Confiabilidad	Materialidad	Probabilidad	Grado de Peligrosidad
	14	Falta de documentación de las aplicaciones o no es satisfactoria	8	8	6	7	5	4	4	42	80	33.6
	16	No existe biblioteca de programas fuentes	7	8	7	7	8	5	5	47	90	42.3
	18	Ausencia de procedimientos de recuperación de aplicaciones en explotación en caso de incidentes	7	8	5	5	9	4	4	42	50	21
	19	Ausencia de controles de seguridad y seguimiento a los usuarios	5	6	4	8	8	7	7	45	80	36
	22	Ausencia de bibliotecas de programas, centro de mantenimiento y de documentación	7	8	5	6	8	5	5	44	75	33
	23	Permiten las copias de seguridad en un plazo satisfactorio resolver todo tipo de fallos?	7	8	7	8	8	5	7	50	75	37.5
	24	Deficiencia en el procedimiento de copias de seguridad en el conjunto software y archivos necesarios para desarrollo y explotación	7	8	8	8	7	7	7	52	75	39
	25	Existen backups en un sitio diferente a la empresa para recuperar el funcionamiento en caso de siniestros	7	8	8	8	8	7	7	53	85	45.05

	26	Ausencia de un programa de reinicio de operaciones en caso de siniestro	6	8	8	6	9	5	5	47	80	37.6
	27	Acceso no autorizado al cuarto del servidor	4	8	5	7	5	7	7	43	75	32.25
	28	Evaluación de controles sobre incendios, inundaciones, interrupciones eléctricas e intrusos	4	7	5	7	7	7	4	41	60	24.6
	33	Existe un encargado de la seguridad en el departamento de sistemas?	5	7	6	7	7	8	5	45	75	33.75
	37	Traumatismo en el reinicio de operaciones por desastre al no contar con plan de contingencias	8	9	7	5	7	5	5	46	90	41.4
	38	Daños y perdidas por falta de un responsable de seguridad física y lógica que dirija y capacite al personal	5	7	6	7	7	7	4	43	65	27.95
	42	Perdida de información por uso no autorizado, divulgación, modificación daño o perdida	4	7	4	7	7	4	3	36	50	18
	53	Acceso de personas no autorizadas a funciones del software, permitiéndoles: leer, modificar, agregar y eliminar datos	8	7	7	8	8	5	8	51	25	12.75
	70	Deficiencia en la documentación de manuales de operaciones y aplicaciones	3	8	5	5	7	3	3	34	65	22.1
	75	El cuarto del servidor es de fácil acceso y no se restringen y controlan las entradas	4	7	5	8	6	4	7	41	55	22.55

	82	Deficiencias en las copias de seguridad de archivos en puestos de trabajo	4	7	5	7	4	4	6	37	60	22.2

2. Definición del plan de contingencias

2.1 Reacción a emergencias

En el evento que un desastre físico extremo ocurra (Incendio total, terremoto, atentados) el siguiente procedimiento será ejecutado:

1. Comunicar a los responsables de ejecutar este procedimiento:
   Ing. Juan Carlos Patiño y/o Ing. Carlos Arturo Rueda
   En el peor de los casos se avisa al Ing. Nelson Mauricio Silva.

2. Preparar centro de computo alterno ubicado en la Carrera 33 No.36-25 teléfono 6456547.

3. Evaluar daños y adquirir el equipo de computo necesario para el reinicio de operaciones. Ver plan de respaldo

4. Configuración del nuevo centro de operaciones, restauración de aplicaciones y datos

5. El proveedor y la asistencia técnica es suministrada por MULTICOMPUTO Calle 45 No. 29-40 PBX 6435340 atención Ing. Liliana Pereira.

En el evento que daños físicos a los componentes de la red ocurran (Daños al servidor, red de comunicaciones) ejecutar el siguiente procedimiento:

1. Notificar a los responsables de restablecer el funcionamiento ing. Juan Carlos Patiño y/o ing. Carlos Arturo Rueda

2. Evaluar situación y determinar daños.

3. Adquirir elementos necesarios para restablecer funcionamiento

4. Configurar los nuevos componentes según características originales (ver documento de configuración del entorno informático)

5. El proveedor y la asistencia técnica es suministrada por MULTICOMPUTO Calle 45 No. 29-40 PBX 6435340 atención Ing. Liliana Pereira

En el evento que los ing. Responsables de ejecutar los anteriores procedimientos se ausenten y su asistencia sea urgente notificar a:

Ing. Nelson Mauricio Silva, residencia Cra. 22 No.31-41 Apto 703 teléfono 6450418 quien se encargara de ejecutar los procedimientos para restablecer el funcionamiento del entorno informático de SEVICOL LTDA.

3. Plan de Respaldo

El responsable del mantenimiento de este plan es el Ing. Carlos Arturo Rueda quien se encargara especialmente de mantener actualizados las copias de seguridad del conjunto aplicaciones y datos semanalmente.

1. El sitio alterno donde se guardaran los elementos de este plan esta ubicado en la Cra. 33 No. 36-25 teléfono 6456547

2. Las aplicaciones a preservar en este lugar por su carácter critico son: Contabilidad, Nomina, Facturación y Cartera

3. En cuanto a las copias de seguridad de aplicaciones y datos se actualizaran semanalmente, cada lunes. Se menciona que Data Ease al efectuar copias de respaldo lo hace tanto de datos como de aplicaciones.

4. En este sitio se mantendrá una copia de la siguiente documentación: Configuración del Entorno Informático de SEVICOL LTDA., copia de esta plan de contingencias y documentación de las aplicaciones.

ANEXO B

CONFIGURACIÓN DEL ENTORNO INFORMATICO DE SEVICOL LTDA

Nombre de la Empresa: SEGURIDAD Y VIGILANCIA COLOMBIANA (SEVICOL LTDA)

1.1 Talento Humano signado a la Función de Sistemas de Información.

1.1.1 Cantidad de personas en el área de Sistemas: 2

1.1.2 Perfil del personal de sistemas.

Perfil	Cantidad
Tecnólogos en Sistemas	
Ingenieros de Sistemas	2
Otros	

1.2 Plataformas de Hardware y Software utilizadas.

Plataforma	Descripción
Sistemas Operacionales	DOS, WINDOWS 95/98/XP, NOVEL NETWARE
Motores de Bases de Datos	DataEase
Otras Herramientas de Desarrollo	Officce para Windows
Software de Red	Novel Netware, Windows
Equipos Activos de la Red	16
Internet	TV Cable Net 24 Horas, TELECON por demanda

Servidores de correo Electrónico	Hosting en American Dominios
Firewalls	VirusScan
E-business	
Servidor	Compaq Proliant 1600

1.3 Sistemas de Información que utiliza la empresa.

Nombre	Módulos Componentes
Sistema de Información para Administrar el Recurso Humano y Contable	Nomina
	Facturación y Cartera
	Contabilidad

1.4 Aplicaciones o Módulos de Sistemas de Información que están en producción y su importancia para la empresa.

No.	Nombre de la aplicación	Importancia para la empresa	Herramienta de desarrollo utilizada	Poseen Programas fuentes?
1	Nomina	Alta	DataEase	Sí
2	Facturación y Cartera	Alta	DataEase	Sí
3	Contabilidad	Alta	DataEase	Sí

1.5 Configuración del Hardware de RED SEVICOL LTDA.

DISPOSITIVO	DESCRIPCIÓN
TECNOLOGÍA	10BASE100
SERVIDOR	COMPAQ PROLIANT 1600
DISCO DURO	2 C/U 10 GB SCSII
MEMORIA RAM	128 MHz
PROCESADOR	PENTIU II 333 MHz
BACKUP	DISCO DURO REMOVIBLE
UPS	3KWA
ESTACIONES DE TRABAJO	17
IMPRESORAS	SANSUG ML 1210 CANTIDAD 3 EPSON DFX 8000 EPSON FX 1170 CANTIDAD 2
CONECTORES	TIPO RJ 45
INTERCONECCIÓN	2 CONCENTRADORES
MEDIO DE TRASNPORTE DE DATOS	CABLEADO UTP 5
SISTEMA OPERATIVO	NOVEL INTRANETWARE V. 4.11 25 USUARIOS
TOPOLOGÍA	TIPO ESTRELLA
SERVIDOR DE IMPRESORAS Y RECURSOS COMPARTIDOS	SERVIDOR DE IMPRESORAS (PC NOMINA) COLA DE DATOS POR NOVEL Y RECURSOS POR

	WINDOWS PC OPERACIONES COLA DE DATOS POR NOVEL
CONTROL DE ACCESO DE COMUNICACIONES	CSMA/CD Carrier Sense with Multiple Acces and Collision Detection

2. ORGANIZACIÓN ADMINISTRATIVA

2.1 COMITÉ ADMINISTRATIVO

GERENTE GENERAL

NOMBRE: **JORGE AURELIO DIAZ**

OBJETIVO DEL CARGO: Representar legalmente la sociedad y ejecutar todos los actos o contratos derivados de la naturaleza de su cargo y que se relacione directamente con el objeto social de la empresa. Usar la firma o razón social, nombrar los empleados que requieran para el normal funcionamiento de la Sociedad y señalar su remuneración, visitar esporádicamente a los clientes para verificar en la fuente la prestación del servicio.

SUBGERENTE

NOMBRE: **SANDRA DIAZ INFANTE**

OBJETIVO DEL CARGO: Velar por el cumplimiento de las metas en la parte administrativa y financiera de la empresa, registrar la información de los cobros dada por los deudores e informar a Tesorería y a la dirección administrativa de las novedades, informar al mensajero de los sitios de recolección de cheques e indagar sobre la gestión realizada por éste, hacer seguimiento a clientes atrasados a través de llamadas, cartas y visitas, análisis de inversiones hechas por la compañía, analizar estados bancarios, pagos pendientes y diferentes propuestas de proveedores, indagar por nuevos contratos, servicios, licitaciones para apoyar la toma de decisiones, atender las solicitudes e información de las diferentes secciones para apoyar el proceso de toma de decisiones, solución de problemas que tengan que ver con el funcionamiento general del empresa.

GERENTE COMERCIAL

NOMBRE: **JUAN CARLOS PATIÑO OROZCO**

OBJETIVO DEL CARGO: Hacer crecer la compañía, basado en análisis reales de mercado y del área financiera.

DIRECTOR ADMINISTRATIVO

NOMBRE: **MARIA ISABEL ALMEIDA**

RESPONSABILIDADES: Llevar a cabo la facturación de la empresa, supervisar el proceso de pago de aportes, supervisar el proceso de nómina, autorizar liquidaciones finales de personal, atención de clientes, estudio y aprobación de préstamos, resolver conflictos administrativos, asegurar el cumplimiento y aplicación de todos los procedimientos administrativos, presentar y sustentar informes a la junta, en reuniones ordinarias de todas las divisiones y en general de la empresa, asistir al comité administrativo, realizar el seguimiento de las licitaciones y cotizaciones presentadas por la compañía, dar soporte en el área de sistemas a toda la organización.

DIRECTOR DE RECURSO HUMANO

NOMBRE: **GILMA PATRICIA DIAZ INFANTE**

RESPONSABILIDADES: Velar por el buen desempeño de recurso humano, garantizar la contratación de personal que cumpla con los perfiles establecidos, integrante del comité disciplinario, tomar la decisión de la elección del nuevo personal de Bucaramanga en el área operativa y administrativa, con base en los resultados del proceso de selección, coordinar el programa de salud ocupacional.

DIRECTOR DE OPERACIONES

NOMBRE: **CP (R) JORGE ENRIQUE GOMEZ SANCHEZ**

RESPONSABILIDADES : Atender las quejas de los clientes a nivel operativo, controlar el movimiento y mantenimiento de armas, radios, relojes, salvoconductos, controlar el trabajo de los supervisores, integrar el comité disciplinario, diligenciar y actualizar los manuales de portería y vigilancia, armamento y comunicaciones para el manejo y control de diferentes equipos y normas de seguridad.

COORDINADOR DE SERVICIOS

NOMBRE: **S.S. ADOLFO LEGUIZAMO**

RESPONSABILIDADES: Ubicar el personal operativo en puestos de trabajo, organizar turnos, apoyar el proceso de nómina, integrar el comité disciplinario, llevar diariamente las planillas de los turnos de trabajo en Bucaramanga, realizar la liquidación del tiempo de trabajo para la liquidación de la nomina de Bucaramanga, registro diario de incapacidades, licencias, permisos, sanciones, nuevos ingresos, entrega de comprobantes de pago y nomina a vigilancia y corroboración del registro, reportar novedades de ingreso, retiros e incapacidades, los días 15 y 30 de cada mes a la secretaria de dirección administrativa para liquidar anticipos y digitar la nomina general.

2.2 SECCION ADMINISTRATIVA

Se encarga de los procesos Facturación, Cartera, Contabilidad, Coordinación de Agencias, Legalización de contratos, Liquidación de aportes, Nómina, Finanzas, Tesorería.

AUXILIAR DE TESORERIA

NOMBRE: **YADIRA CUBILLOS**

RESPONSABILIDADES: Elaborar los comprobantes y cheques correspondientes a los pagos de proveedores autorizados siguiendo los procedimientos establecidos los días viernes y/o miércoles, realizar cheques y comprobantes de egreso al personal, acumular y suministrar la información de las consignaciones realizadas y extractos bancarios a tiempo para la realización de la conciliación, ingresar al sistema las facturas que se elaboran a maquina, descargar en el sistema las facturas canceladas por los clientes o actualizar en el sistema la cartera en el momento que realizan los pagos, realizar el listado de la cartera y suministrar dicha información actualizada a la subgerencia, realizar el informe diario de tesorería de efectivo disponible los lunes y los jueves, archivar los comprobantes de egreso, funciones que sean asignadas por los jefes y que sean afines con la naturaleza del cargo.

SECRETARIA JURÍDICA Y ALMACENISTA

NOMBRE: **NIDIA LUZ CAMACHO**

RESPONSABILIDADES: Realizar la planilla de las horas trabajadas en los respectivos puestos, llevar el control de los comprobantes de egreso de los prestamos hechos al personal, registrar la cantidad del descuento por conceptos de prestamos y otros descuentos por cada vigilante antes de la nomina, recepción y archivo de cartas, terminación de contrato, renuncia o cancelación de contrato, notificar a los guardas implicados en caso de descargo, elaboración de planillas de nomina del personal y grabar los turnos a cada guarda, control y pago de embargos del personal notificado, controlar y grabar los descuentos del personal en el proceso de nomina, realizar el control de cardex para saber con que dotación se cuenta y tomar decisiones pertinentes de compra, dotar al nuevo personal con dos uniformes completos de acuerdo al puesto, llevar el registro en los formatos asignados para el proceso de compras en el sistema de gestión de calidad, solicitar a la superintendencia los números asignados a la empresa y mandarlas elaborar.

SECRETARIA AUXILIAR CONTABLE

NOMBRE: **ANA LUCIA JURADO**

RESPONSABILIDADES: Revisar el listado de las retenciones hechas a los proveedores, facilitar la información para el calculo de la retención en la fuente al Estado por parte del revisor fiscal, sacar listados para el informe de la superintendencia los primeros 5 días del mes, del personal activo hasta la fecha,

digitar recibos de caja y notas contables de aportes, nominas y ajustes, listar balances, cuadros y flujos para licitaciones o para créditos bancarios, realizar conciliaciones bancarias, digitar los cuadros y balances financieros, suministrar información segura y confiable de la retención en la fuente que realizan los clientes, los primeros meses del año, causar los gastos del mes según facturas de proveedores, realizar el proceso de llevar la facturación y recibos de caja de cartera al área de contabilidad, elaboración del formulario para el pago de IVA SES, elaboración de formularios para declaración de renta y patrimonio para SEVICOL y sus socios, digitar la nomina del personal administrativo, imprimir informes de fecha de ingreso de personal, crear código a clientes nuevos para la facturación, imprimir y revisar el pago de retención en la fuente.

AUXILIAR DE SEGURIDAD SOCIAL

NOMBRE: **ESPERANZA TRIANA DE JAIMES**

RESPONSABILIDADES: Vinculación de personal a EPS, ARP, EFP, Caja de compensación, manejo de incapacidades, con la documentación, ingresar al sistema, e ingresar el nombre y número de cuenta al sistema del nuevo personal y reingresos, hacer el cobro a la EPS de incapacidad por enfermedad, asegurarse que el personal este en el sistema con su respectiva seguridad social, apoyar el proceso de liquidación de aportes.

SECRETARIA DE DIRECCIÓN ADMINISTRATIVA

NOMBRE: **SANDRA MILENA ESTUPIÑÁN**

RESPONSABILIDADES: Apoyar a la Dirección Administrativa en todos sus procesos tales como Nomina, Facturación y Contabilidad.

RECEPCIONISTA

NOMBRE: **MARIA CONSUELO RODRIGUEZ**

RESPONSABILIDADES: Brindar una imagen excelente de la empresa, atención del cliente interno y externo, contestar el teléfono, transferir la llamada o recibir y hacer llegar el mensaje a quien corresponda.

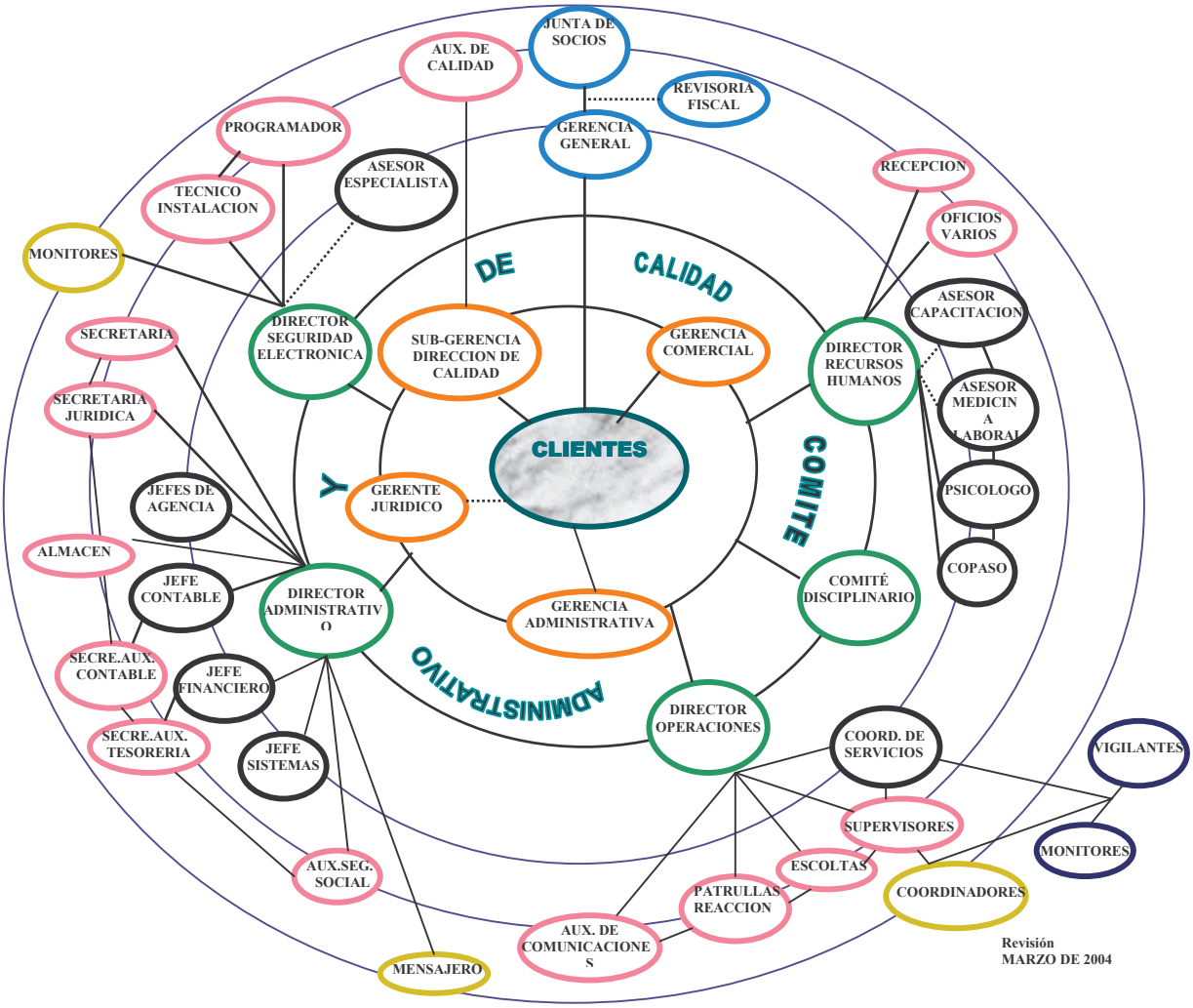
2.3 SECCION OPERATIVA

Ejecuta y coordina el desarrollo del objeto social de la empresa, a través de los supervisores, escoltas, coordinadores y vigilantes, orientados por el Director de este departamento, estableciendo procedimientos operativos a nivel proactivo y reactivo para cubrir las necesidades del cliente en Seguridad Integral.

2.4 SECCION DE SEGURIDAD ELECTRÓNICA

Conformada por el Director, monitores y Grupo de reacción motorizada. Contempla la instalación, mantenimiento y monitoreo de alarmas, a los usuarios.

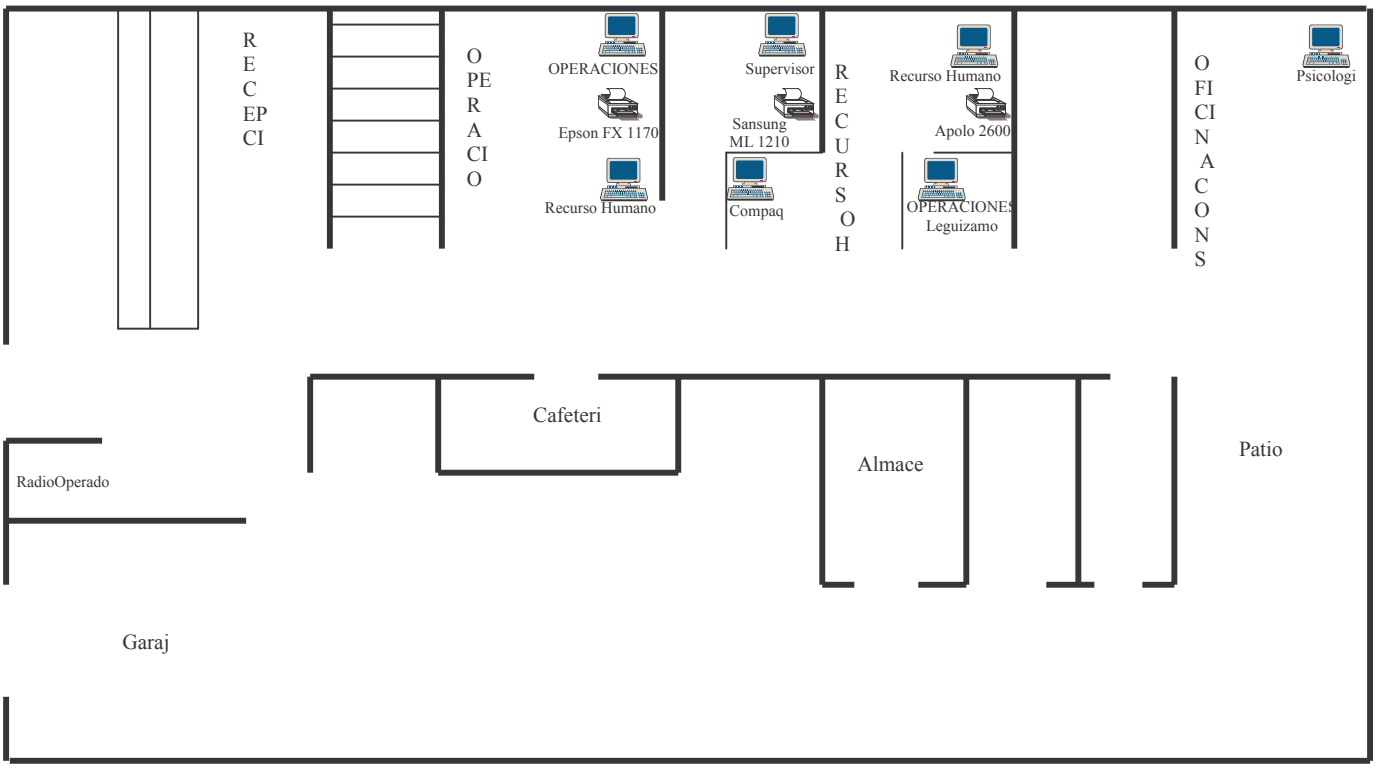
3. Organigrama SEVICOL LTDA.



4. Planos de locaciones de la empresa

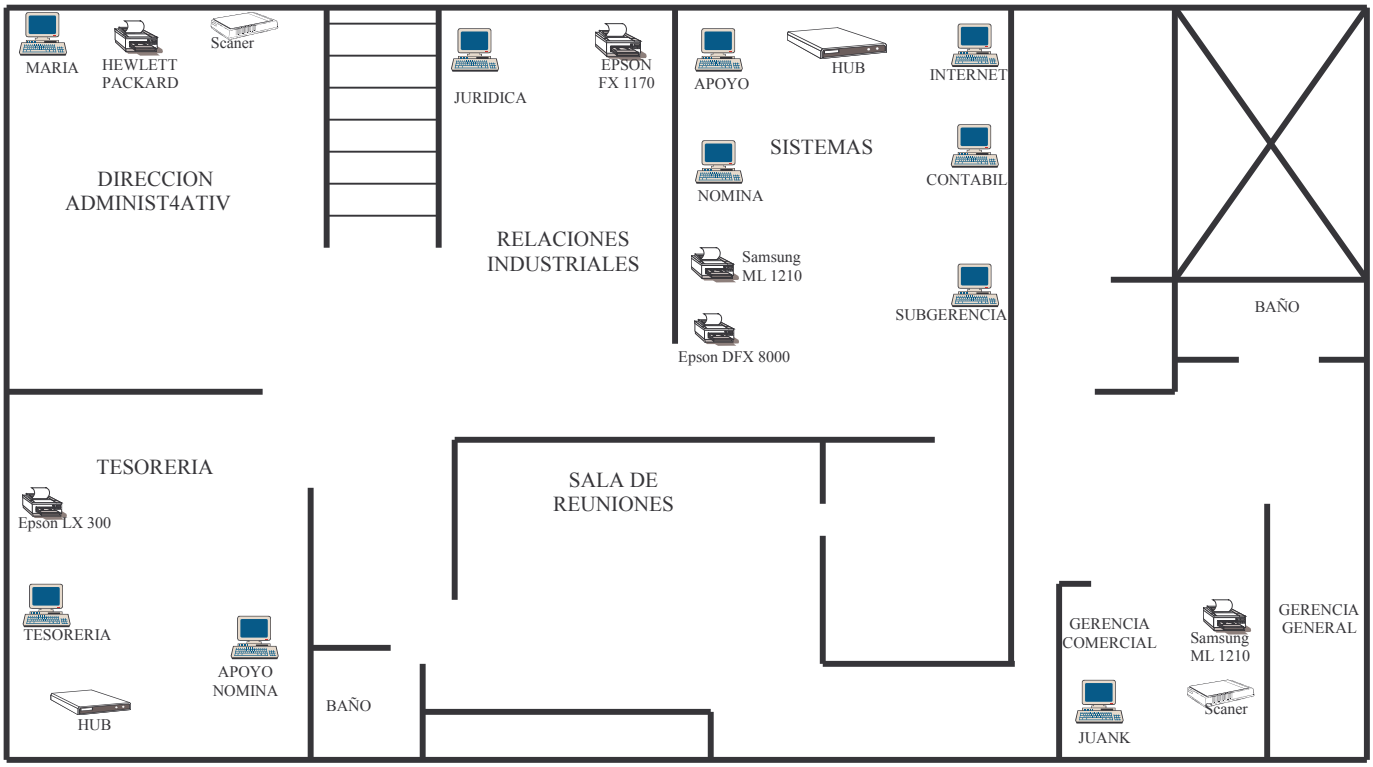
CONFIGURACION DEL ENTORNO INFORMATICO DE SEVICOL LTDA

PRIMER PISO



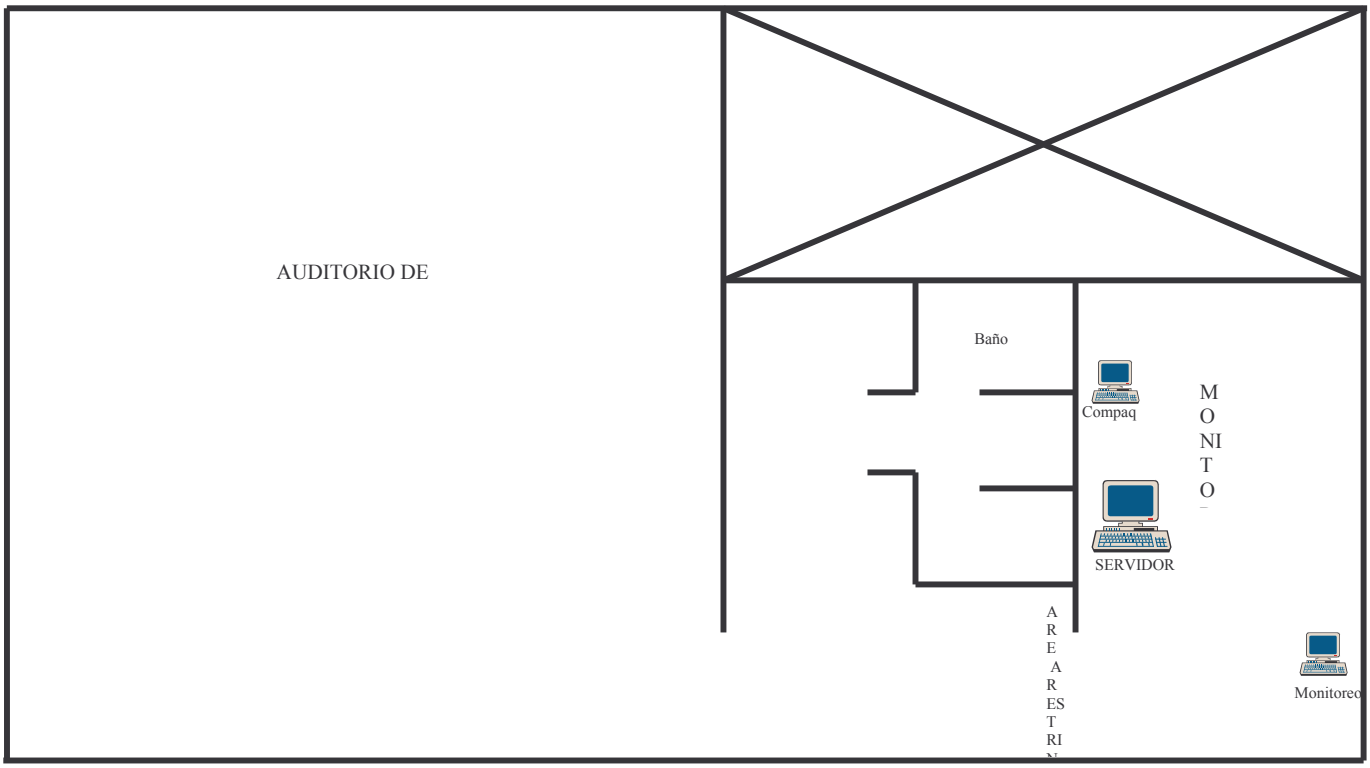
CONFIGURACION DEL ENTORNO INFORMATICO DE SEVICOL LTDA

SEGUNDO PISO

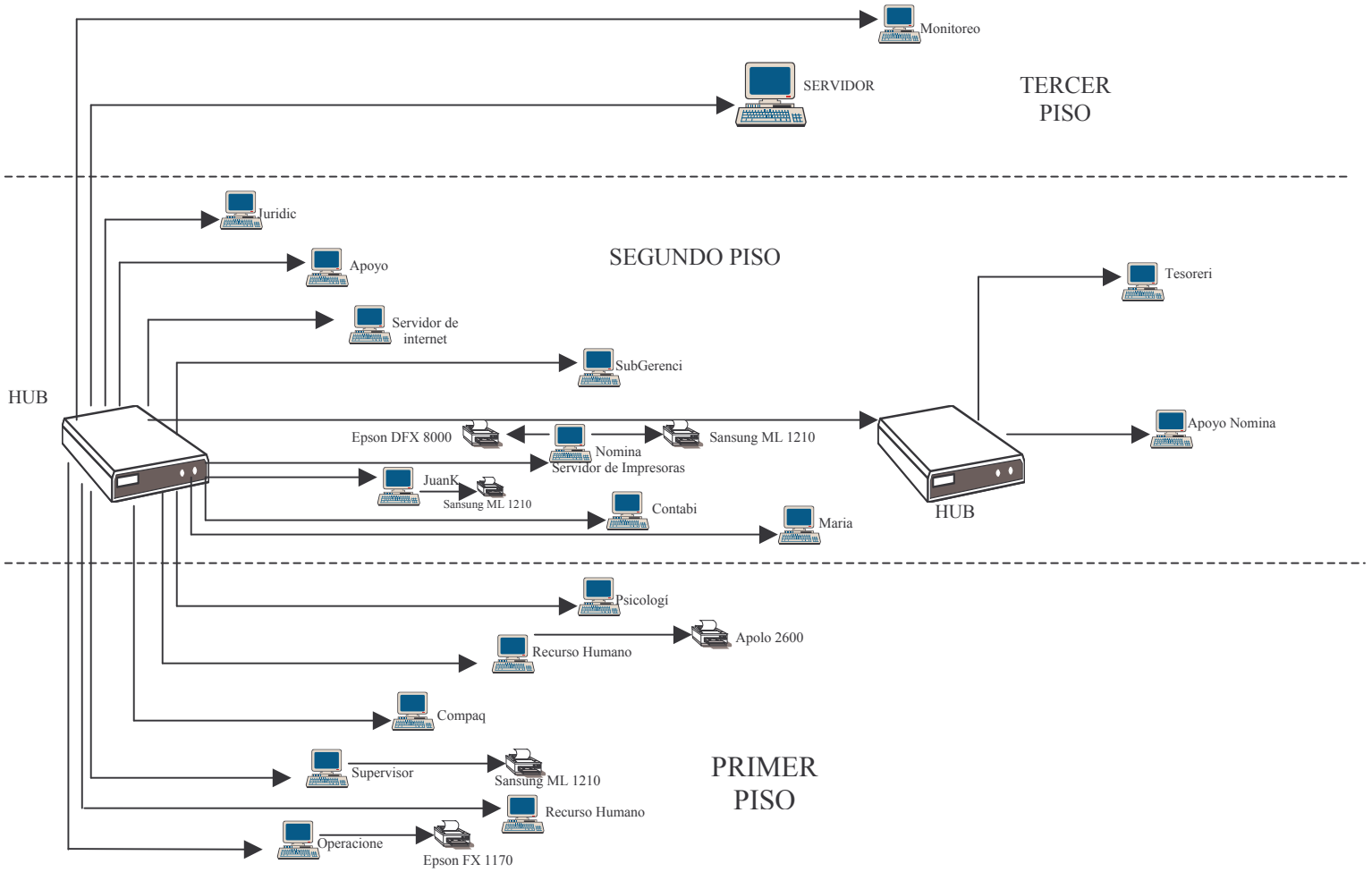


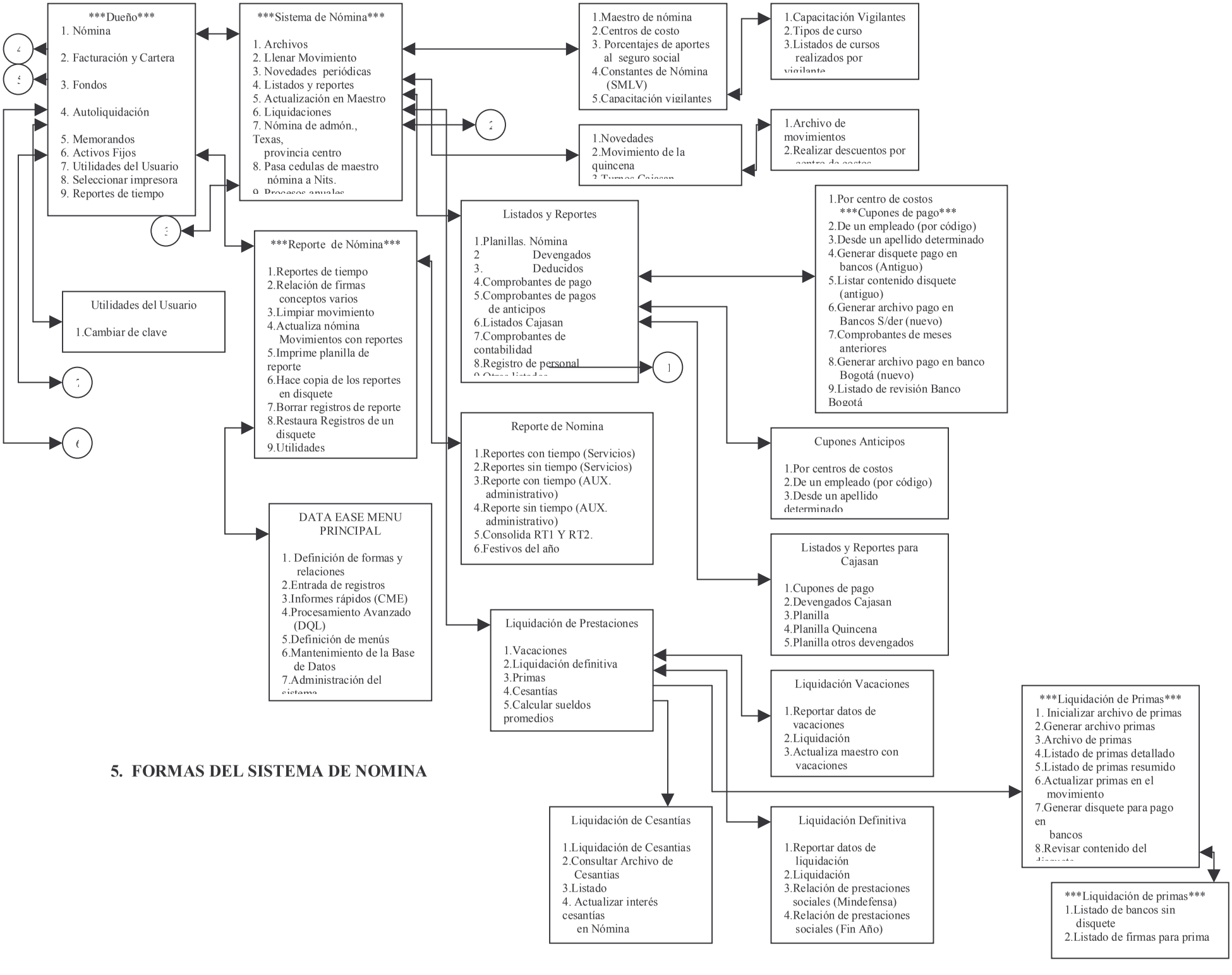
CONFIGURACION DEL ENTORNO INFORMATICO DE SEVICOL LTDA

TERCER PISO

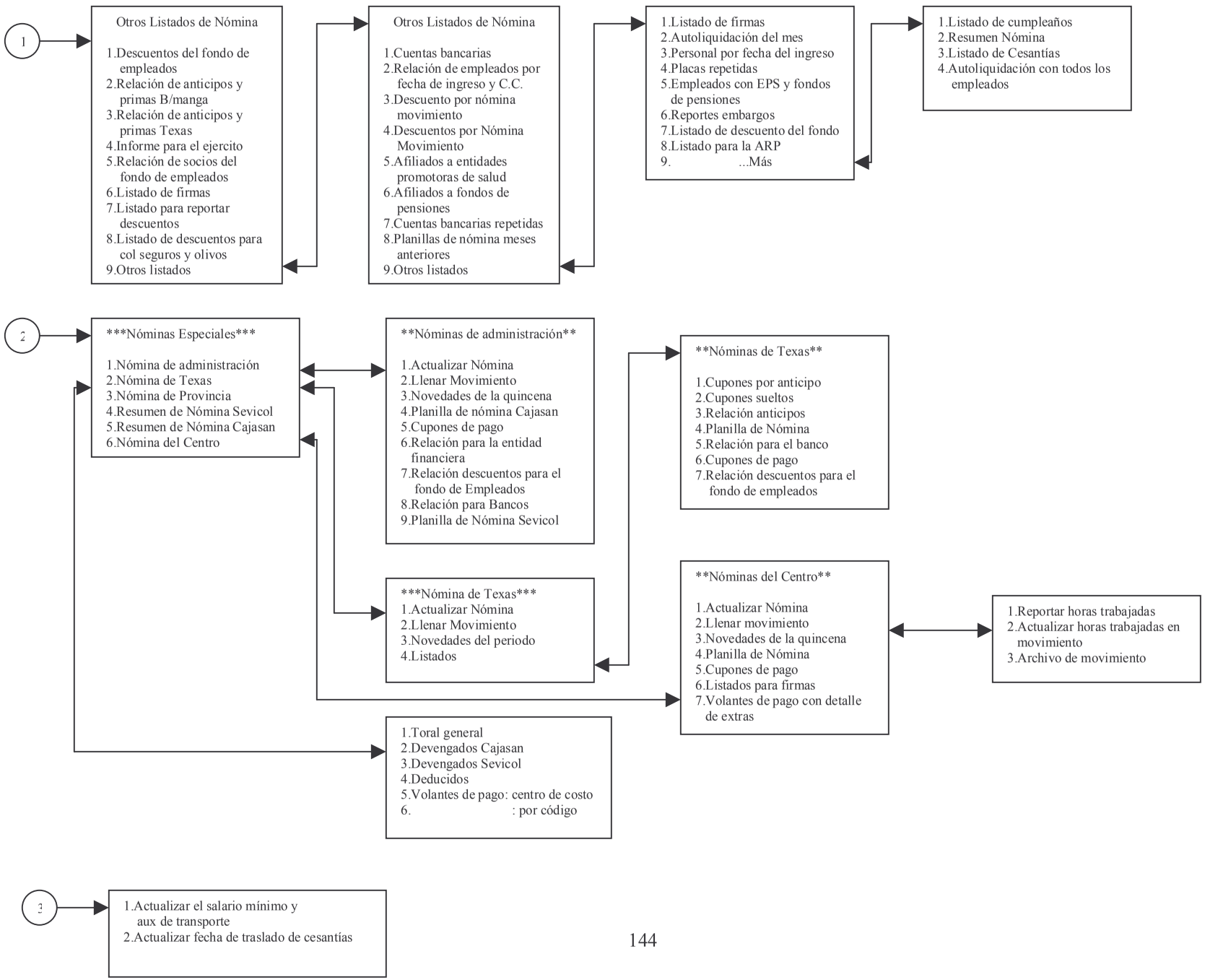


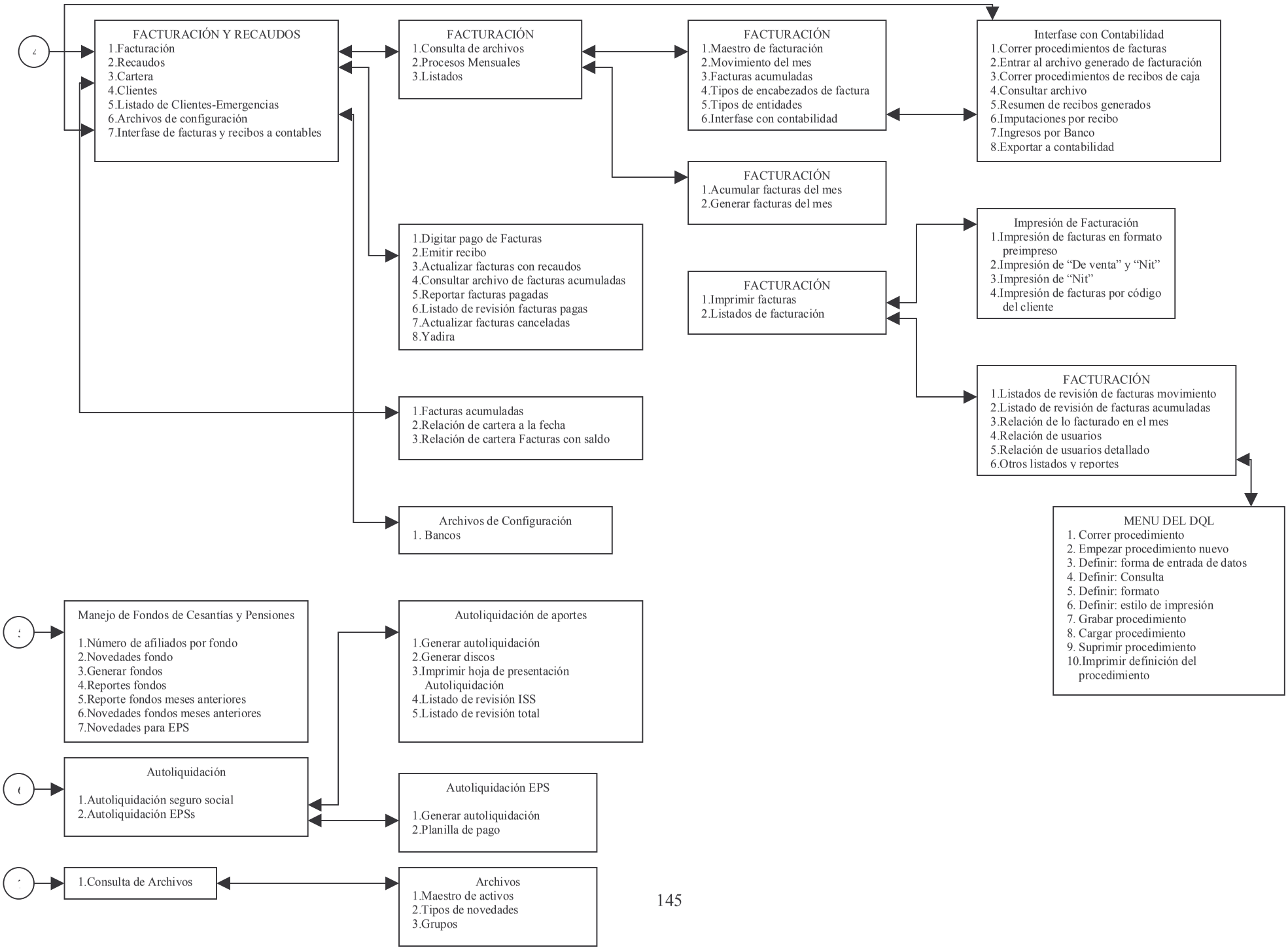
CONFIGURACION FISICA DE LA RED DE SEVICOL LTDA

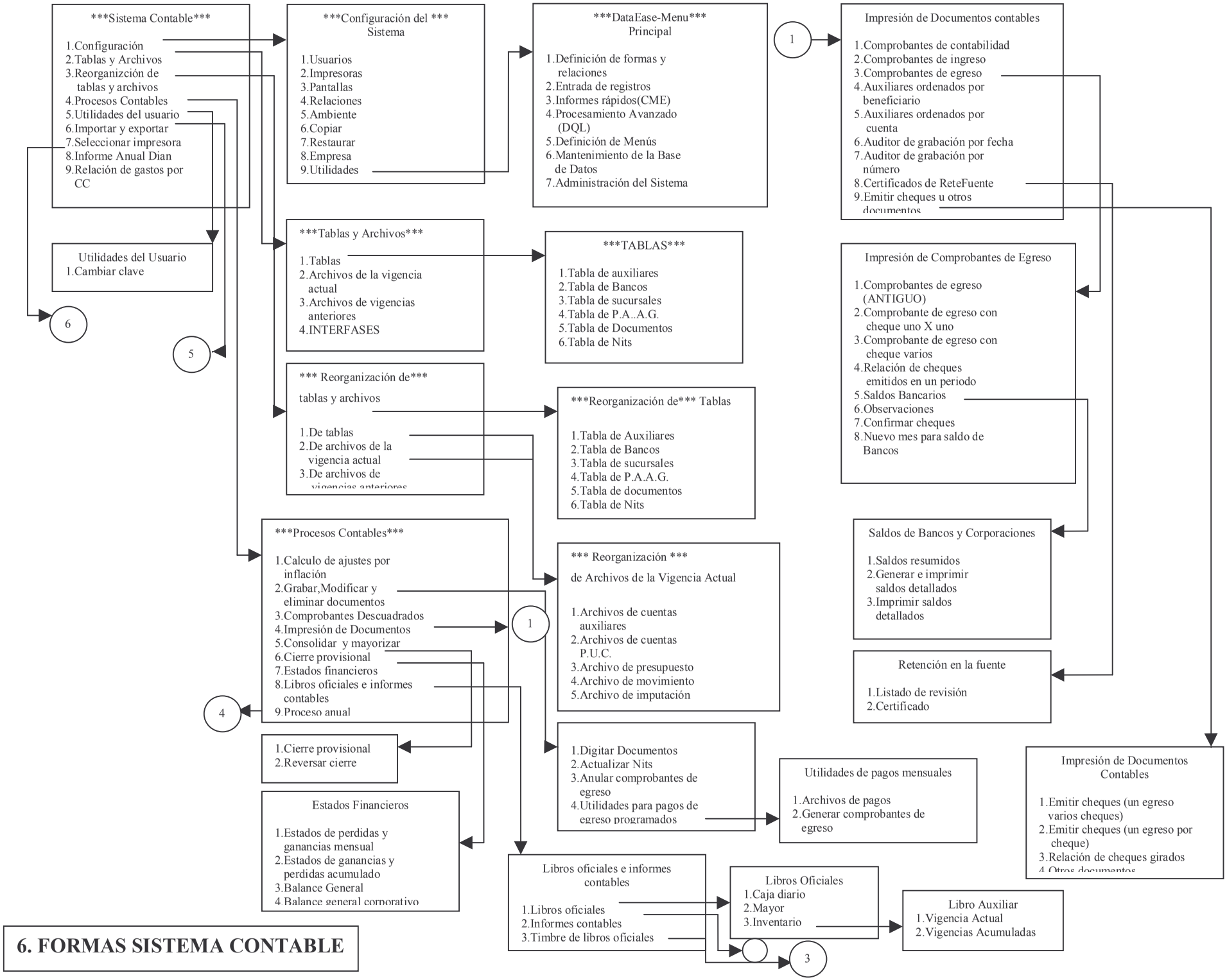




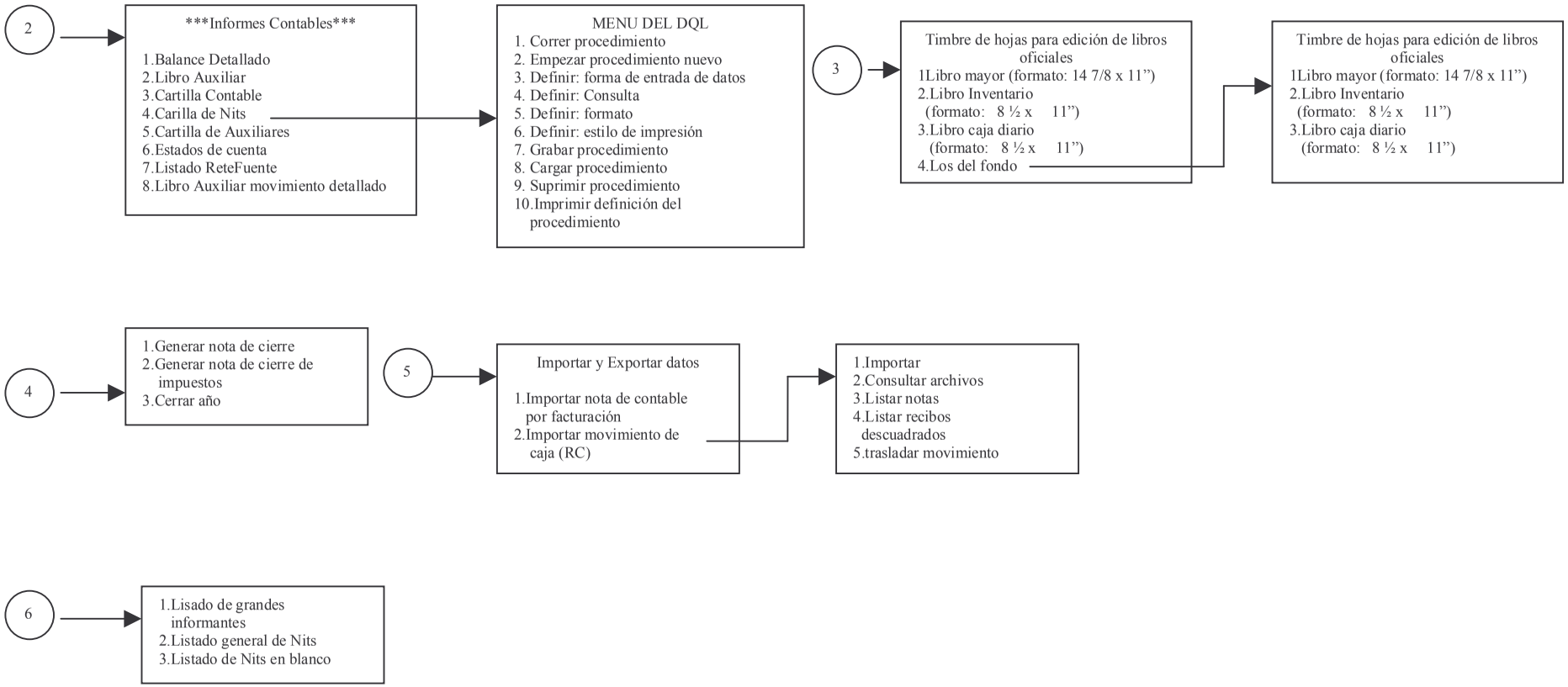
5. FORMAS DEL SISTEMA DE NOMINA


1
Otros Listados de Nómina
1.Descuentos del fondo de empleados
2.Relación de anticipos y primas B/manga
3.Relación de anticipos y primas Texas
4.Informe para el ejercito
5.Relación de socios del fondo de empleados
6.Listado de firmas
7.Listado para reportar descuentos
8.Listado de descuentos para col seguros y olivos
9.Otros listados
Otros Listados de Nómina
1.Cuentas bancarias
2.Relación de empleados por fecha de ingreso y C.C.
3.Descuento por nómina movimiento
4.Descuentos por Nómina Movimiento
5.Afiliados a entidades promotoras de salud
6.Afiliados a fondos de pensiones
7.Cuentas bancarias repetidas
8.Planillas de nómina meses anteriores
9.Otros listados
1.Listado de firmas
2.Autoliquidación del mes
3.Personal por fecha del ingreso
4.Placas repetidas
5.Empleados con EPS y fondos de pensiones
6.Reportes embargos
7.Listado de descuento del fondo
8.Listado para la ARP
9. ...Más
1.Listado de cumpleaños
2.Resumen Nómina
3.Listado de Cesantías
4.Autoliquidación con todos los empleados
2
Nóminas Especiales
1.Nómina de administración
2.Nómina de Texas
3.Nómina de Provincia
4.Resumen de Nómina Sevicol
5.Resumen de Nómina Cajasan
6.Nómina del Centro
Nóminas de administración
1.Actualizar Nómina
2.Llenar Movimiento
3.Novedades de la quincena
4.Planilla de nómina Cajasan
5.Cupones de pago
6.Relación para la entidad financiera
7.Relación descuentos para el fondo de Empleados
8.Relación para Bancos
9.Planilla de Nómina Sevicol
Nóminas de Texas
1.Cupones por anticipo
2.Cupones sueltos
3.Relación anticipos
4.Planilla de Nómina
5.Relación para el banco
6.Cupones de pago
7.Relación descuentos para el fondo de empleados
Nómina de Texas
1.Actualizar Nómina
2.Llenar Movimiento
3.Novedades del periodo
4.Listados
Nóminas del Centro
1.Actualizar Nómina
2.Llenar movimiento
3.Novedades de la quincena
4.Planilla de Nómina
5.Cupones de pago
6.Listados para firmas
7.Volantes de pago con detalle de extras
1.Reportar horas trabajadas
2.Actualizar horas trabajadas en movimiento
3.Archivo de movimiento
1.Toral general
2.Devengados Cajasan
3.Devengados Sevicol
4.Deducidos
5.Volantes de pago: centro de costo
6. : por código
3
1.Actualizar el salario mínimo y aux de transporte
2.Actualizar fecha de traslado de cesantías


FACTURACIÓN Y RECAUDOS
1.Facturación
2.Recaudos
3.Cartera
4.Clientes
5.Listado de Clientes-Emergencias
6.Archivos de configuración
7.Interfase de facturas y recibos a contables
FACTURACIÓN
1.Consulta de archivos
2.Procesos Mensuales
3.Listados
FACTURACIÓN
1.Maestro de facturación
2.Movimiento del mes
3.Facturas acumuladas
4.Tipos de encabezados de factura
5.Tipos de entidades
6.Interfase con contabilidad
Interfase con Contabilidad
1.Correr procedimientos de facturas
2.Entrar al archivo generado de facturación
3.Correr procedimientos de recibos de caja
4.Consultar archivo
5.Resumen de recibos generados
6.Imputaciones por recibo
7.Ingresos por Banco
8.Exportar a contabilidad
FACTURACIÓN
1.Acumular facturas del mes
2.Generar facturas del mes
1.Digitar pago de Facturas
2.Emitir recibo
3.Actualizar facturas con recaudos
4.Consultar archivo de facturas acumuladas
5.Reportar facturas pagadas
6.Listado de revisión facturas pagas
7.Actualizar facturas canceladas
8.Yadira
Impresión de Facturación
1.Impresión de facturas en formato preimpreso
2.Impresión de “De venta” y “Nit”
3.Impresión de “Nit”
4.Impresión de facturas por código del cliente
FACTURACIÓN
1.Imprimir facturas
2.Listados de facturación
1.Facturas acumuladas
2.Relación de cartera a la fecha
3.Relación de cartera Facturas con saldo
FACTURACIÓN
1.Listados de revisión de facturas movimiento
2.Listado de revisión de facturas acumuladas
3.Relación de lo facturado en el mes
4.Relación de usuarios
5.Relación de usuarios detallado
6.Otros listados y reportes
Archivos de Configuración
1. Bancos
MENU DEL DQL
1. Correr procedimiento
2. Empezar procedimiento nuevo
3. Definir: forma de entrada de datos
4. Definir: Consulta
5. Definir: formato
6. Definir: estilo de impresión
7. Grabar procedimiento
8. Cargar procedimiento
9. Suprimir procedimiento
10.Imprimir definición del procedimiento
Manejo de Fondos de Cesantías y Pensiones
1.Número de afiliados por fondo
2.Novedades fondo
3.Generar fondos
4.Reportes fondos
5.Reporte fondos meses anteriores
6.Novedades fondos meses anteriores
7.Novedades para EPS
Autoliquidación de aportes
1.Generar autoliquidación
2.Generar discos
3.Imprimir hoja de presentación Autoliquidación
4.Listado de revisión ISS
5.Listado de revisión total
Autoliquidación
1.Autoliquidación seguro social
2.Autoliquidación EPSs
Autoliquidación EPS
1.Generar autoliquidación
2.Planilla de pago
1.Consulta de Archivos
Archivos
1.Maestro de activos
2.Tipos de novedades
3.Grupos



6. FORMAS SISTEMA CONTABLE


2
Informes Contables
1.Balance Detallado
2.Libro Auxiliar
3.Cartilla Contable
4.Carilla de Nits
5.Cartilla de Auxiliares
6.Estados de cuenta
7.Listado ReteFuente
8.Libro Auxiliar movimiento detallado
MENU DEL DQL
1. Correr procedimiento
2. Empezar procedimiento nuevo
3. Definir: forma de entrada de datos
4. Definir: Consulta
5. Definir: formato
6. Definir: estilo de impresión
7. Grabar procedimiento
8. Cargar procedimiento
9. Suprimir procedimiento
10.Imprimir definición del procedimiento
3
Timbre de hojas para edición de libros oficiales
1Libro mayor (formato: 14 7/8 x 11")
2.Libro Inventario (formato: 8 ½ x 11")
3.Libro caja diario (formato: 8 ½ x 11")
4.Los del fondo
Timbre de hojas para edición de libros oficiales
1Libro mayor (formato: 14 7/8 x 11")
2.Libro Inventario (formato: 8 ½ x 11")
3.Libro caja diario (formato: 8 ½ x 11")
4
1.Generar nota de cierre
2.Generar nota de cierre de impuestos
3.Cerrar año
5
Importar y Exportar datos
1.Importar nota de contable por facturación
2.Importar movimiento de caja (RC)
1.Importar
2.Consultar archivos
3.Listar notas
4.Listar recibos descuadrados
5.trasladar movimiento
6
1.Lisado de grandes informantes
2.Listado general de Nits
3.Listado de Nits en blanco