República de Cuba

Ministerio de Educación Superior

Instituto Superior Minero Metalúrgico

Dr. Antonio Núñez Jiménez

Facultad de Humanidades
Departamento de Contabilidad y Finanzas

Trabajo de Diploma

***Título**: Auditoria Informática del Sistema de Gestión BaaN.*

***Autor**: Yanisa Peña Columbie*

***Tutores:** Msc. Marcos Medinas.*
Msc. Rafael Zamora .

***Consultante:** Ing. Iliana Driggs Pérez.*

Moa, junio del 2006
"Año de la Revolución Energética en Cuba"

Carta de Autorización del Autor.

Se autoriza al Departamento de Contabilidad y Finanzas del Instituto Superior Minero Metalúrgico, "Dr. Antonio Núñez Jiménez" a utilizar toda la información contenida en este trabajo de diploma.

_____

Yanisa Peña Columbie

DEDICATORIA

Dedico este trabajo a quienes con su luz iluminaron el camino para que pudiera llegar hasta el final, va dedicada:

A mi hija Amanda Rachel por su cariño y apoyo en todo momento.

A ti mi amor por tanto cariño y estar siempre a mi lado.

A mi Madre por estar al tanto del progreso de mi investigación.

En especial a mi Abuela, que con su apoyo diario me enseñó el camino que debía transitar y sobre todo por ser la mejor madre del mundo.

Yanisa

AGRADECIMIENTOS

Se que agradecer va más allá de una página y unas escasas letras, espero que la vida me de la oportunidad de mostrar mi agradecimiento de una forma más profunda, de todas formas quiero darle gracias a mis padres y mi abuela, mi familia, a mi amor Osvaldo que siempre ha estado al lado de su hija y por su apoyo incondicional, a Martha, Iliana, Rafael Zamora; pues sin su ayuda no lo hubiera podido lograr y a mi amiga Tania que una vez más puedo contar con ella, a todos mis compañeros de trabajo que siempre me han apoyado ante cualquier situación. En fin, gracias a todos los que me motivaron y apoyaron para poder realizar este sueño materializado.

Yanisa

“ Mucho hemos aprendido y mucho más seguiremos aprendiendo.
Nuevas fuentes de ingreso surgen y el rigor en la administración de los recursos deberá incrementarse.
Viejos y nuevos malos hábitos deberán ser erradicados.
La eterna vigilancia es el precio de la honradez y la eficiencia” .

Fidel Castro Ruz

"… Tenemos que hacer análisis del los costos cada vez más detallados que nos permitan aprovechar hasta la última partícula de trabajo que se pierden del hombre….."

Ernesto Che Guevara.

RESUMEN

El software BaaN es un Sistema Integrado de Gestión que se encuentra en funcionamiento en la Empresa “Comandante Pedro Sotto Alba” – Moa Nickel S.A. En él se contabilizan todas las operaciones de la empresa y es importante garantizar que las mismas sean correctas y que se reflejen adecuadamente los hechos económicos.

El objetivo de este trabajo consiste en realizar una Auditoria Informática (AI) para la evaluación y diagnóstico integral del módulo BaaN- Finanzas, para evaluar si el ambiente de procesamiento genera una información financiera confiable. Se auditó el período desde el 1 de Enero al 31 de Diciembre del 2005.

Se llevó a cabo una prueba al ciclo de seguridad de derechos a los usuarios al Módulo BaaN Finanzas, utilizando el software CRMR. Se prepararon formularios, se realizaron entrevistas, se calcularon y ponderaron secciones, segmentos y subsecciones, se identificaron las áreas mejorables.

Se realizó el ejercicio de evaluación de los controles generales del sistema informático y se evaluaron cualitativamente los riesgos, determinándose que los mismos operaron de manera efectiva durante el periodo auditado, y que realizan de manera confiable el procesamiento de la información financiera de la empresa, existiendo una confianza razonable en la información que se obtiene del ambiente de procesamiento.

Se identificaron mejoras a aplicar para robustecer el control en el ambiente de procesamiento en general. Se efectuaron personalizaciones, que aportaron un valor adicional al trabajo realizado.

INDICE

INTRODUCCION

El 90 por ciento de las Empresas tienen toda su información estructurada en Sistemas Informáticos, los cuales se han constituido en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial: Los Sistemas de Información y Gestión de la Empresa.

La función contable es validada por el uso de un sistema de información confiable, que cumpla las normas y estándares propios de la actividad, garantizando que la información sea la adecuada para reflejar la posición económica y financiera de la empresa y para ayudar a la toma de decisiones.

El **Objeto de Estudio** es el software denominado BaaN , el cual es un sistema integrado de gestión que se encuentra en funcionamiento en la empresa "Comandante Pedro Sotto Alba" – Moa Nickel S.A. desde el 1º de Julio del 2002. En él se contabilizan todas las operaciones de la empresa y cuenta con 14 módulos que integran la gestión y control de inventarios, proyectos, compras, mantenimiento y todas las operaciones de registro contable, de forma interactiva, que permiten el seguimiento y control en las operaciones fundamentales.

El **Problema Científico** radica en la necesidad de asegurar que el sistema brinde una información contable y financiera confiable y optimizar el uso de sus potencialidades para ayudar a la toma de decisiones.

El **Campo de Acción**: Es él módulo BaaN de Finanzas donde se realizan las operaciones contables y financieras.

El **Objetivo General:** de este trabajo consiste en la realizar una Auditoria Informática (AI) para la evaluación y diagnóstico integral del sistema informático de

gestión BaaN que permita determinar si el ambiente de procesamiento genera información financiera confiable.

La **hipótesis** planteada es que si se logra auditar profundamente y revisar el rendimiento de nuestro sistema, identificaremos sus debilidades y se demostrará si este contribuye a un control interno efectivo y al procesamiento de la información acorde a las Normas Contables Cubanas.

Los **objetivos específicos** consisten en :

- Conocer y documentar la infraestructura y funciones de los módulos contables y financieros de BaaN.
- Revisar el cumplimiento de las normas de seguridad, confiabilidad y compartimentación de la información.
- Revisar el cumplimiento de las políticas de la empresa referentes a la Información para el sistema BaaN.
- Planificar, organizar, ejecutar e informar la auditoria de sistema.
- Realizar pruebas de auditorias del Ciclo de Seguridad de derechos de los Usuarios en BaaN y los Controles Generales del Sistema Informático.

Para el desarrollo de la investigación se utilizaran varios métodos científicos tales como análisis-síntesis de la información recopilada relacionada con la temática investigada, métodos computacionales de programación funcional, método inductivo para los análisis teóricos realizados, método teórico de la modelación.

Este trabajo consiste en dos capítulos. El capitulo I es la fundamentación teórica conceptual de la auditoria informática (AI) y en el capítulo II se aborda el desarrollo de la auditoria Informática al sistema de Gestión BaaN.

CAPITULO I. FUNDAMENTACION TEORICA CONCEPTUAL DE LA AUDITORIA INFORMATICA.

1.1 Descripción Conceptual de la Auditoria.

El término Auditoria se ha empleado incorrectamente con frecuencia, ya que se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas. El concepto de auditoria es mucho más que esto. Es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una sección, un organismo, una entidad, etc.

La palabra auditoria proviene del latín *auditorius,* y de esta proviene la palabra auditor, que se refiere a todo aquel que tiene la virtud de oír.

Por otra parte, el Diccionario Español lo define como: Revisor de Cuentas colegiado. En un principio esta definición carece de la explicación del objetivo fundamental que persigue todo auditor: Evaluar la eficiencia y eficacia. Boletín de Normas de Auditoria del Instituto Mexicano de contadores nos dice que: "La auditoria no es una actividad meramente mecánica que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevados a cabo son de carácter indudable."

De todo esto se puede decir que la auditoria es un examen crítico pero no mecánico, que no implica la preexistencia de fallas en la entidad auditada y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo.

El Decreto Ley No. 159 Manual del Auditor (MAC): define la Auditoria como un proceso sistemático, que consiste en obtener y evaluar objetivamente evidencias sobre las afirmaciones relativas a los actos o eventos de carácter económico – administrativo, con el fin de determinar el grado de correspondencia entre esas afirmaciones y los criterios establecidos, para luego comunicar los resultados a las personas interesadas. Se practica por profesionales calificados e independientes de la organización, en conformidad con normas y procedimientos técnicos.

Finalmente citamos la definición que aparece en el Manual del Auditor (MAC), la cual define la auditoria como: Examen objetivo, crítico, sistemático y selectivo de las políticas, normas, prácticas, procedimientos y procesos para dictaminar respecto a la economía, eficiencia y eficacia de la utilización de los recursos informáticos; la integridad, confiabilidad, oportunidad y validez de la información y la efectividad de los controles en las áreas, las aplicaciones, los sistemas de redes u otros vinculados a la actividad informática.

1.2 Tipos de Auditorias

- Auditoria Financiera.
- Auditoria Operativa.
- Auditoria Fiscal.
- Auditoria Informática.
- Auditoria Externa.
- Auditoria Interna.

La auditoria interna se realiza con recursos materiales y humanos que pertenecen a la empresa auditada. La auditoria interna existe por expresa decisión de la Empresa, o sea, que puede optar por su disolución en cualquier momento y tiene la ventaja de que puede actuar periódicamente realizando revisiones globales, como parte de su Plan Anual y de su actividad normal. Los auditados conocen estos planes y se habitúan a las auditorias, especialmente cuando las consecuencias de las recomendaciones encontrada benefician su trabajo.

La auditoria interna se define como el control que se desarrolla como instrumento de la propia administración y consiste en una valoración independiente de sus actividades; que comprende el examen de los sistemas de control interno, de las operaciones contables y financieras y de la aplicación de las disposiciones administrativas y legales que corresponda; con la finalidad de mejorar el control y

grado de autonomía, eficiencias y eficacias en la utilización de los recursos; prevenir el uso indebido de éstos y coadyuvar al fortalecimiento de la disciplina en general.

La auditoria externa es realizada por personas afines a la empresa auditada. Se presupone una mayor objetividad que en la Auditoria Interna, debido al mayor distanciamiento entre auditores y auditados.

Se define como el examen o verificación de las transacciones, cuentas, informaciones, o estados financieros, correspondientes a un período, evaluando la conformidad o cumplimiento de las disposiciones legales o internas vigentes en el sistema de control interno contable. Se practica por profesionales facultados, que no son empleados de la organización cuyas afirmaciones o declaraciones auditan.

Además, examina y evalúa la planificación, organización, dirección y control interno administrativo, la economía y eficiencia con que se han empleado los recursos humanos, materiales y financieros, así como el resultado de las operaciones previstas a fin de determinar si se han alcanzado las metas propuestas.

En cuanto a empresas se refiere, solamente las más grandes pueden poseer una Auditoria propia y permanente, mientras que el resto acuden a las auditorias externas. Puede ser que algún profesional informático sea trasladado desde su puesto de trabajo a la Auditoria Interna de la empresa cuando ésta existe. Hoy, existe un Departamento de Informática dentro de la misma empresa con un elevado grado de autonomía.

Una empresa o institución que posee auditoria interna puede y debe en ocasiones contratar servicios de auditoria externa. Las razones para hacerlo suelen ser: Necesidad de auditar una materia de gran especialización, para la cual los servicios propios no están suficientemente capacitados.

Aunque la auditoria interna sea independiente del Departamento de Sistemas, sigue formando parte de la misma empresa, por lo que es necesario que se le realicen auditorias externas como para tener una visión independiente la empresa.

Auditoria Informática: es la que evalúa los controles de la función Informática, analizar la eficiencia de los sistemas, verificar el cumplimiento de las políticas y procedimientos de la empresa y revisar que los recursos materiales y humanos de esta área se utilicen eficientemente. El auditor informático debe velar por la correcta utilización de los recursos que la empresa dispone para lograr un eficiente y eficaz Sistema de Información(SI).

1.3 Objetivos de la Auditoria Informática

Los principales objetivos de la Auditoria Informática (AI) es : el control de la función informática, el análisis de las eficiencias de los Sistemas Informáticos que comporta, la verificación del cumplimiento de la Normativa General de la Empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos e informáticos. Los Sistemas Informáticos afrontan varios inconvenientes que hacen necesaria la realización de la **Auditoria de Sistemas**.

Auditoria de Sistemas: es la verificación de controles en el procesamiento de la información, desarrollo de sistemas e instalación con el objetivo de evaluar su efectividad y presentar recomendaciones a la empresa. Dentro de los **objetivos tenemos**:

- Incrementar la satisfacción de los usuarios de los sistemas computarizados
- Asegurar una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles.
- Conocer la situación actual del área informática y las actividades y esfuerzos necesarios para lograr los objetivos propuestos.

Las computadoras y los Centros de Proceso de Datos (CPD) se convirtieron en blancos apetecibles no solo para el espionaje, sino para la delincuencia y el terrorismo. En este caso interviene la Auditoria Informática de Seguridad.

Un Sistema Informático (SI) mal diseñado puede convertirse en una herramienta peligrosa para la Empresa; como consecuencia de que las máquinas obedecen ciegamente a las órdenes recibidas.

1.4 Alcance de la Auditoria Informática.

El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la Auditoria Informática (AI) y se complementa con los objetivos de ésta. El alcance ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado, hasta que punto se ha llegado, y cuales materias fronterizas han sido omitidas.

Control de integridad de registros: Hay aplicaciones que comparten registros, son registros comunes. Si una aplicación no tiene integrado un registro común, cuando lo necesite utilizar no lo va encontrar y, por lo tanto, la aplicación no funcionaría como debería.

- Control de validación de errores: *S*e corrobora que el sistema que se aplica para detectar y corregir errores sea eficiente.

1.5 Caracterización de la Auditoria Informática.

La información de la entidad, es importante, se ha convertido en un Activo Real de la misma, como sus Inventarios o materias primas si las hay. Por ende, han de realizarse inversiones informáticas, actividad de la que se ocupa la *Auditoria de Inversión Informática*. Del mismo modo, los Sistemas Informáticos han de protegerse de modo global y particular; a ello se debe la existencia de la *Auditoria de Seguridad*

Informática en general, o a la auditoria de seguridad de alguna de sus áreas, como pudieran ser Desarrollo o Técnica de Sistemas.

Cuando se producen cambios estructurales en la Informática, se reorganiza de alguna forma su función: y obedece al campo de la *Auditoria de Organización Informática.*

Estos tres tipos de auditorias informática engloban a las actividades auditoras que se realizan en una auditoria parcial. De otra manera; cuando se realiza una auditoria del área de Desarrollo de Proyectos de la Informática de una Empresa, es porque en ese desarrollo existen, además de ineficiencias, debilidades de organización, o de inversiones, o de seguridad, o alguna mezcla de ellas.

- **Síntomas de Necesidad de la Auditoria Informática (AI)**

Las Empresas acuden a las auditorias externas cuando existen síntomas bien perceptibles de debilidades. Estos síntomas pueden agruparse en clases:

1. **Síntomas de descoordinación y desorganización**

- No coinciden los objetivos de la Informática de la Empresa y las de la propia Empresa.
- Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente.
- Puede ocurrir que con algún cambio masivo de personal, o en una reestructuración fallida de alguna área o en la modificación de alguna Norma importante

2. **Síntomas de mala imagen e insatisfacción de los usuarios**

- No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de Software en los terminales de usuario, refrescamiento de paneles, variación de los ficheros que deben ponerse diariamente a su disposición.

- No se reparan las averías de Hardware, ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.
- No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de aplicaciones críticas y sensibles.

3. Síntomas de debilidades económico-financiero

- Incremento desmesurado de costos.
- Necesidad de justificación de Inversiones Informáticas (la empresa no está absolutamente convencida de tal necesidad y decide obtener opiniones de diferentes fuentes).
- Desviaciones Presupuestarias significativas.
- Costos y plazos de nuevos proyectos (deben auditarse simultáneamente a Desarrollo de Proyectos y al órgano que realizó la petición).

4. Síntomas de Inseguridad

- Evaluación de nivel de riesgos
- Seguridad Lógica
- Seguridad Física
- Confidencialidad

Los datos son propiedad inicialmente de la organización que los genera. Continuidad del Servicio. Es un concepto aún más importante que la Seguridad. Establece las estrategias de continuidad entre fallos mediante Planes de Contingencia Totales y Locales.

Centro de Proceso de Datos fuera de control. Si tal situación llegara a percibirse, sería prácticamente inútil la auditoria. Esa es la razón por la cual, en este caso, el síntoma debe ser sustituido por el mínimo indicio.

1.5.1 Divisiones de Auditoria Informática.

El departamento de Informática posee una actividad proyectada al exterior, al usuario, aunque el "exterior" siga siendo la misma empresa. He aquí, la *Auditoria Informática de Usuario*. Se hace esta distinción para contraponerla a la informática interna, en donde se hace la informática cotidiana y real. En consecuencia, existe una *Auditoria Informática de Actividades Internas*.

El control del funcionamiento del departamento de informática con el exterior, con el usuario; se realiza por medio de la Dirección. Su figura es importante, en tanto en cuanto es capaz de interpretar las necesidades de la Empresa. Una informática eficiente y eficaz requiere el apoyo continuo de su Dirección frente al "exterior". Revisar estas interrelaciones constituye el objeto de la *Auditoria Informática de Dirección*. Estas tres auditorias, mas la Auditoria de Seguridad, son las cuatro Áreas Generales de la Auditoria Informática más importantes.

Dentro de las áreas generales, se establecen las siguientes **Divisiones de Auditoria Informática**: de Explotación, de Sistemas, de Comunicaciones y de Desarrollo de Proyectos. Estas son las Áreas Especificas de la Auditoria Informática (AI) más importantes.

Áreas Específicas	**Áreas Generales**			
	Interna	Dirección	Usuario	Seguridad
Explotación				
Desarrollo				
Sistemas				
Comunicaciones				
Seguridad				

Cada Área Específica puede ser auditada desde los siguientes criterios generales:

- Desde su propio funcionamiento interno.
- Desde el apoyo que recibe de la Dirección y, en sentido ascendente, del grado de cumplimiento de las directrices de ésta.
- Desde la perspectiva de los usuarios, destinatarios reales de la informática.
- Desde el punto de vista de la seguridad que ofrece la Informática en general o la rama auditada.

Estas combinaciones pueden ser ampliadas y reducidas según las características de la empresa auditada.

Operatividad es una función de rendimiento consistente en que la organización y las maquinas funcionen. No es admisible detener la maquinaria informática para descubrir sus fallos y comenzar de nuevo. La auditoria debe iniciar su actividad cuando los Sistemas están operativos, es el principal objetivo, el de mantener tal situación.

La operatividad de los Sistemas ha de constituir entonces la principal preocupación del auditor informático. Para conseguirla hay que acudir a la realización de *Controles Técnicos Generales de Operatividad* y *Controles Técnicos Específicos de Operatividad*, previos a cualquier actividad del mismo.

Los Controles Técnicos Generales son los que se realizan para verificar la compatibilidad de funcionamiento simultaneo del Sistema Operativo y el Software de base con todos los subsistemas existentes, así como la compatibilidad del Hardware y del Software instalados. Estos controles son importantes en las instalaciones que cuentan con varios competidores, debido a que la profusión de entornos de trabajo muy diferenciados obliga a la contratación de diversos productos de Software básico, con el consiguiente riesgo de abonar más de una vez el mismo producto o desaprovechar parte del Software abonado. Puede ocurrir también con los productos de Software básico desarrollados por el personal de Sistemas Interno, sobre todo cuando los diversos equipos están ubicados en Centros de Proceso de Datos

geográficamente alejados. Lo negativo de esta situación es que puede producir la inoperatividad del conjunto. Cada Centro de Proceso de Datos tal vez sea operativo trabajando independientemente, pero no será posible la interconexión e intercomunicación de todos los Centros de Proceso de Datos si no existen productos comunes y compatibles.

Los Controles Técnicos Específicos, de modo menos acusado, son igualmente necesarios para lograr la Operatividad de los Sistemas. Un ejemplo de lo que se puede encontrar mal son parámetros de asignación automática de espacio en disco que dificulten o impidan su utilización posterior por una Sección distinta de la que lo generó. También, los periodos de retención de ficheros comunes a varias Aplicaciones pueden estar definidos con distintos plazos en cada una de ellas, de modo que la pérdida de información es un hecho que podrá producirse con facilidad, quedando inoperativa la explotación de alguna de las Aplicaciones mencionadas.

Revisión de Controles de la Gestión Informática

Una vez conseguida la Operatividad de los Sistemas, el segundo objetivo de la auditoria es la verificación de la observancia de las normas teóricamente existentes en el departamento de Informática y su coherencia con las del resto de la Empresa. Para ello, habrán de revisarse sucesivamente y en este orden:

Las Normas Generales de la Instalación Informática. Se realizará una revisión inicial sin estudiar a fondo las contradicciones que pudieran existir, pero registrando las áreas que carezcan de normativa, y sobre todo verificando que esta Normativa General Informática no está en contradicción con las Normas Generales informáticas de la empresa.

Los Procedimientos Generales Informáticos. Se verificará su existencia, al menos en los sectores más importantes. Por ejemplo, la recepción definitiva de las máquinas deben estar firmada por los responsables de su Explotación y el alta de nueva

Aplicaciones se podría producirse de no existir los Procedimientos de Backup y Recuperación correspondientes.

a) Auditoria Informática de Producción o Explotación:

La Explotación Informática se ocupa de producir resultados informáticos de todo tipo: listados impresos, ficheros soportados magnéticamente para otros informáticos, ordenes automatizadas para lanzar o modificar procesos industriales. La explotación informática se puede considerar como un proceso con ciertas peculiaridades que la distinguen de las reales. Para su realización la Explotación Informática se dispone de una materia prima, los datos, que es necesario transformar, y que se someten previamente a controles de integridad y calidad. La transformación se realiza por medio del Proceso Informático, el cual está dirigido por los programas. Obteniéndose el producto final, que son sometidos a varios controles de calidad y, finalmente, son distribuidos al cliente o usuario.

Auditar Explotación: consiste en auditar las secciones que la componen y sus interrelaciones. La Explotación Informática se divide en tres grandes áreas: Planificación, Producción y Soporte Técnico, en la que cada cual esta formado por varios grupos.

- **Control de Entrada de Datos:**

Se analiza la captura de la información en soporte compatible con los Sistemas, el cumplimiento de plazos y calendarios de tratamientos y entrega de datos; la correcta transmisión de datos entre entornos diferentes. Se verifica que los controles de integridad y calidad de datos se realizan de acuerdo a Norma.

- **Planificación y Recepción de Aplicaciones:**

Se audita las normas de entrega de Aplicaciones por parte de Desarrollo, verificando su cumplimiento y su calidad de interlocutor único. Debe realizarse muestreos selectivos de la Documentación de las Aplicaciones explotadas. Se inquirirá sobre la

anticipación de contactos con desarrollo para la planificación a mediano y largo plazo.

- **Centro de Control y Seguimiento de Trabajos:**

Se analiza cómo se prepara, se lanza y se sigue la producción diaria. Básicamente, la explotación Informática ejecuta procesos por cadenas o lotes sucesivos (Batch), o en tiempo real (Tiempo Real). Mientras que las Aplicaciones de Teleproceso están permanentemente activas y la función de Explotación se limita a vigilar y recuperar incidencias, el trabajo Batch absorbe una buena parte de los efectivos de Explotación. En muchos Centros de Proceso de Datos, éste órgano recibe el nombre de Centro de Control de Batch. Este grupo determina el éxito de la explotación, es uno de los factores más importantes en el mantenimiento de la producción.

- **Batch y Tiempo Real:**

Las Aplicaciones Batch son aquellas que contienen mucha información durante el día y en la noche se corre un proceso enorme que hace relacionar toda la información, calcular transacciones y obtener resultados, por ejemplo: reportes. O sea, recolecta información durante el día, sin ser sometidas a procesos. Es solamente un tema de "Data Entry" que recolecta información, corre el proceso Batch (por lotes), y calcula todo lo necesario para arrancar al día siguiente.

Las Aplicaciones que son Tiempo Real u Online, son las que, una vez ingresada la información correspondiente, procesadas inmediatamente y devuelven un resultado. Son Sistemas que tienen que responder en Tiempo Real.

- **Centro de Control de Red y Centro de Diagnostico:**

El Centro de Control de Red suele ubicarse en el área de producción de Explotación. Sus funciones se refieren exclusivamente al ámbito de las comunicaciones, estando muy relacionado con la organización de Software de Comunicaciones de Técnicas de Sistemas. Debe analizarse la fluidez de esa relación y el grado de coordinación entre ambos. Se verificará la existencia de un punto focal único, desde el cual sean perceptibles todos las líneas asociadas al sistema. El Centro de Diagnosis es donde

se atienden las llamadas de los usuarios-clientes que han sufrido averías o incidencias, tanto de Software como de Hardware. El Centro de Diagnostico está especialmente indicado para informáticos y con usuarios dispersos en un amplio territorio. Es uno de los elementos que contribuyen a configurar la imagen de la Informática de la Empresa. Debe ser auditada desde esta perspectiva, desde la sensibilidad del usuario sobre el servicio de que dispone. No basta con comprobar la eficiencia técnica del Centro, es necesario analizarlo simultáneamente en el ámbito de Usuario.

b) Auditoria Informática de Desarrollo de Proyectos o Aplicaciones:

La función de Desarrollo es una evolución del llamado Análisis y Programación de Sistemas y Aplicaciones. A su vez, engloba muchas áreas, tantas como sectores informatizables tiene la empresa. Muy escuetamente, una Aplicación recorre las siguientes fases:

- Prerrequisitos del Usuario y del entorno
- Análisis funcional
- Diseño
- Análisis orgánico (Reprogramación y Programación)
- Pruebas
- Entrega a Explotación y alta para el Proceso.

Estas fases deben estar sometidas a un exigente control interno en, caso contrario, los costos pueden excederse y puede producirse la insatisfacción del usuario. La auditoria cual deberá comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la máquina sean exactamente los previstos y a los solicitados inicialmente.

Una auditoria de aplicaciones pasa indefectiblemente por la observación y el análisis de cuatro consideraciones:

a. *Revisión de las metodologías utilizadas*: Se analiza éstas, de modo que se asegure la modularidad de las posibles futuras ampliaciones de la Aplicación y el fácil mantenimiento de las mismas.
b. *Control interno de las aplicaciones*: se debe revisar las mismas fases que presuntamente han debido seguir el área correspondiente de Desarrollo:
c. Estudio de Vialidad de la Aplicación. Importante para Aplicaciones largas, complejas y caras.
d. Definición Lógica de la Aplicación. Se analizan los postulados lógicos de actuación, en función de la metodología elegida y la finalidad que persigue el proyecto.
e. Desarrollo Técnico de la Aplicación. Se verifica que éste sea ordenado y correcto. Las herramientas técnicas utilizadas en los diversos programas deben ser compatibles.
f. Diseño de Programas. Debe poseer la máxima sencillez, modularidad y economía de recursos.
g. Métodos de Pruebas. Se realiza de acuerdo a las Normas de la Instalación. Se utiliza juegos de ensayo de datos, sin que sea permisible el uso de datos reales.
h. Documentación. Cumplió la Normativa establecida en la Instalación, tanto la de Desarrollo como la de entrega de Aplicaciones a Explotación.
i. Equipo de Programación. Deben fijarse las tareas de análisis puro, de programación y las intermedias. En Aplicaciones complejas se producirían variaciones en la composición del grupo, pero estos deberán estar previstos.

- ***Satisfacción de usuarios:***

Una Aplicación técnicamente eficiente y bien desarrollada, se considera fracasada si no sirve a los intereses del usuario que la solicitó. La aquiescencia del usuario proporciona grandes ventajas posteriores, ya que evitará reprogramaciones y disminuirá el mantenimiento de la aplicación.

- ***Control de Procesos y Ejecuciones de Programas Críticos:***

El auditor no debe descartar la posibilidad de que se esté ejecutando un módulo que no se corresponde con el programa fuente que desarrolló, codificó y probó el área de

Desarrollo de Aplicaciones. Se ha de comprobar la correspondencia biunívoca y exclusiva entre el programa codificado y su compilación. Si los programas fuente y los programas módulos no coincidieran podrían provocar, desde errores de bulto que producirían graves y altos costos de mantenimiento, hasta fraudes, pasando por acciones de sabotaje, espionaje industrial-informativo. Por ende, hay normas muy rígidas en cuanto a las Librerías de programas; aquellos programas fuente que hayan sido dados como buenos por Desarrollo, son entregados a Explotación.
Se realizan los siguientes pasos:
1.- Se copia el programa fuente en la Librería de Fuentes de Explotación, a la que nadie más tiene acceso.
2.- Se compila y se instala el programa, depositándolo en la Librería de Módulos de Explotación, a la que nadie más tiene acceso.
3.- Se copian los programas fuentes que les sean solicitados para modificarlos, arreglarlos, etc. en el lugar que se le indique. Cualquier cambio exigirá pasar nuevamente por el punto 1.

Como el sistema de auditar y dar el alta a una nueva Aplicación es bastante ardua y compleja, se utiliza un sistema llamado U.A.T (User Acceptance Test). Este consiste en que el futuro usuario de esta Aplicación use los mismos programas como si la estuviera usando en Producción para que detecte por sí solos los errores de la misma. Estos defectos que se encuentran se van corrigiendo a medida que se va haciendo el U.A.T. Una vez que se consigue el U.A.T., el usuario tiene que dar su aprobación. Todo este proceso tiene que ser controlado, es necesario evaluar que la prueba sea correcta, que exista un plan de prueba, que esté involucrado tanto el cliente como el desarrollador y que estos defectos se corrijan, que todo el sistema sea comprobado y que todos los U.A.T. estén aprobados por el usuario.

b) Auditoria Informática de Sistema:

Se ocupa de analizar la actividad que se conoce como técnica de sistemas en todas sus facetas. Hoy, la importancia creciente de las telecomunicaciones ha propiciado

que las Comunicaciones, Líneas y Redes de las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de Sistemas.

- **Sistemas Operativos:**

Engloba los Subsistemas de Teleproceso, Entrada / Salida. Debe verificarse en primer lugar que los Sistemas están actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera. El análisis de las versiones de los Sistemas Operativos permite descubrir las posibles incompatibilidades entre otros productos de Software Básico adquiridos por la instalación y determinadas versiones de aquellas. Deben revisarse los parámetros variables de las Librerías más importantes de los Sistemas, por si difieren de los valores habituales aconsejados por el constructor.

- **Software Básico:**

Es fundamental para el auditor conocer los productos de software básico que han sido facturados aparte de la propia computadora. Por razones económicas y por razones de comprobación si la computadora podría funcionar sin el producto adquirido por el cliente. El caso del Software desarrollado por el personal informático de la empresa, el auditor debe verificar que éste no agreda ni condiciona al sistema. Igualmente, debe considerar el esfuerzo realizado en términos de costos, de existir alternativas más económicas.

- **Software de Teleproceso (Tiempo Real):**

No se incluye en Software Básico por su especialidad e importancia. Las consideraciones anteriores son válidas para éste también.

- **Tunning:**

Es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los Sistema y Subsistemas del conjunto. Las acciones de tunning deben diferenciarse de los controles habituales que realiza el personal de Técnica de Sistemas. El tunning posee una naturaleza más revisora,

estableciéndose previamente planes y programas de actuación según los síntomas observados. Se pueden realizar: Cuando existe sospecha de deterioro del comportamiento parcial o general del sistema o de modo sistemático y periódico, por ejemplo cada 6 meses. En este caso sus acciones son repetitivas y están planificados y organizados de antemano.

El auditor debe conocer el número de Tunning realizados en el último año, así como sus resultados. Debe analizar los modelos de carga utilizados y los niveles e índices de confianza de las observaciones.

- **Optimización de los Sistemas y Subsistemas:**

Técnica de Sistemas debe realizar acciones permanentes de optimización como consecuencia de la realización de tunnings preprogramados o específicos. El auditor verificará que las acciones de optimización fueron efectivas y no comprometieron la Operatividad de los Sistemas ni el plan crítico de producción diaria de Explotación.

Optimización:

Por ejemplo: Referido a la instalación de una aplicación, normalmente está vacía, no tiene nada cargado adentro. Lo que puede suceder es que, a medida que se va cargando, esta disminuye la velocidad. Debido a que todas las referencias a tablas se hace cada vez mayor, la información que está moviendo aumenta, entonces la Aplicación se tiende a poner lenta. Lo que se tiene que hacer es un análisis del desempeño, para luego optimizarla, mejorar su rendimiento.

- **Administración de Base de Datos:**

El diseño de las Bases de Datos, se ha convertido en una actividad muy compleja y sofisticada, por lo general desarrollada en el ámbito de Técnica de Sistemas, y de acuerdo con las áreas de Desarrollo y usuarios de la empresa. Al conocer el diseño y arquitectura de éstas por parte de Sistemas, se les encomienda también su administración. Los auditores de Sistemas han observado algunas disfunciones derivadas de la relativamente escasa experiencia que Técnica de Sistemas tiene sobre la problemática general de los usuarios de Bases de Datos.

La administración tendría que estar a cargo de Explotación. El auditor de Base de Datos debe asegurarse que Explotación conoce suficientemente las que son accedidas por los Procedimientos que ella ejecuta. Analizará los Sistemas de salvaguarda existentes, que competen igualmente a Explotación. Revisará finalmente la integridad y consistencia de los datos, así como la ausencia de redundancias entre ellos.

- **Investigación y Desarrollo:**

Como existen Empresas que utilizan y necesitan de informáticas desarrolladas, saben que sus propios efectivos están desarrollando aplicaciones que son concebidas inicialmente para su uso interno, pueden ser susceptibles de adquisición por otras empresas, haciendo competencia a las Empresas del ramo. La auditoria informática deberá cuidar de que la actividad de Investigación y Desarrollo no interfiera ni dificulte las tareas fundamentales internas.

La propia existencia de aplicativos para la obtención de estadísticas desarrollados por los técnicos de Sistemas de la empresa auditada, y su calidad, proporcionan al auditor experto una visión bastante exacta de la eficiencia y estado de desarrollo de los Sistemas.

d) Seguridad de operaciones en el ambiente de las redes de datos.

Se prohíbe la conexión de las máquinas donde se procese información clasificada a las redes de datos de alcance global.

Son de obligatoria implementación los mecanismos de seguridad de los cuales están provistas las redes de datos; así como de aquellos que permitan filtrar o depurar la información que se intercambie, de acuerdo a los intereses predeterminados por cada una de ellas.

e) Auditoria de la Seguridad informática.

La computadora es un medio que contiene gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. Expuesta a robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar: el llamado "virus" de las computadoras, el cual, aunque tiene diferentes intenciones, se encuentra principalmente para paquetes que son copiados sin autorización ("piratas") y borra toda la información disponible en un disco. Al auditar los sistemas se debe considerar tener cuidado que no existan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus. El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica. La seguridad física se refiere a la protección del Hardware y los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales.

La seguridad lógica se refiere a la seguridad de uso del software, la protección de los datos, procesos y programas, así como el ordenado y autorizo de acceso de los usuarios a la información.

Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el

acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Estos paquetes han sido populares desde hace muchos años en el mundo de las computadoras grandes, y los principales proveedores ponen a disposición de clientes algunos de estos paquetes.

La seguridad informática se divide en Area General y como Area Específica (seguridad de explotación, seguridad de las aplicaciones, etc.). Así, se podrán efectuar auditorias de la Seguridad Global de una Instalación Informática –Seguridad General- y auditorias de la Seguridad de un área informática determinada Seguridad Especifica.

Con el incremento de agresiones a instalaciones informáticas en los últimos años, se han ido originando acciones para mejorar la Seguridad Informática a nivel físico. Los accesos y conexiones indebidos a través delas Redes de Comunicaciones, han acelerado el desarrollo de productos de Seguridad lógica y la utilización de sofisticados medios criptográficos.

El sistema integral de seguridad debe comprender:

- Elementos administrativos
- Definición de una política de seguridad
- Organización y división de responsabilidades
- Seguridad física y contra catástrofes(incendio, terremotos, etc.)
- Prácticas de seguridad del personal
- Elementos técnicos y procedimientos
- Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.
- Aplicación de los sistemas de seguridad, incluyendo datos y archivos
- El papel de los auditores, tanto internos como externos
- Planeación de programas de desastre y su prueba.
- La decisión de abordar una Auditoria Informática de Seguridad Global en una empresa, se fundamenta en el estudio cuidadoso de los riesgos potenciales a

los que está sometida. Se elaboran "matrices de riesgo", en donde se consideran los factores de las "Amenazas" a las que está sometida una instalación y los "Impactos" que aquellas puedan causar cuando se presentan. Las matrices de riesgo se representan en cuadros de doble entrada Amenaza-Impacto, en donde se evalúan las probabilidades de ocurrencia de los elementos de la matriz.

1.6 Técnicas Empleadas en la Auditoria Informática.

Las técnicas empleadas para realizar una auditoria informática son las siguientes:

- **Cuestionarios:**

Las auditorias informáticas (AI) se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Para esto, suele ser lo habitual comenzar solicitando el llenado de cuestionarios preimpresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar.

Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes muy específicos en cada situación, y muy cuidados en su fondo y su forma. Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoria. Cabe aclarar, que esta primera fase puede omitirse cuando los auditores hayan adquirido por otro medios la información que aquellos preimpresos hubieran proporcionado.

- **Entrevistas:**

El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:

- Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.
- Mediante "entrevistas" en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.
- Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca finalidades concretas.

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas en cuestionarios.
Aparte de algunas cuestiones menos importantes, la entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo. El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de preguntas variadas y sencillas. No obstante, esta sencillez es solo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada.

- **Lista de Chequeo (Checklists)*.***

El auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis posterior, lo cual no significa que someta al auditado a preguntas estereotipadas que no conducen a nada. Muy por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para la cumplimentación sistemática de sus Cuestionarios, de sus Checklists.

Hay opiniones que descalifican el uso de las Checklists, ya que consideran que leerle conjunto aplicando la memoria o leídas en alta voz descalifica al auditor informático. Esto no es usar Checklists, es una evidente falta de profesionalismo. Para lograrlo se prefiere de proceso interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente.
El conjunto de estas preguntas recibe el nombre de Checklist. Salvo excepciones, las Checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

Según la claridad de las preguntas y el talento del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable. El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer.

Por ello, aun siendo importante tener elaborados los cuestionarios o listas de preguntas muy sistematizados, coherentes y clasificados por materias, aun lo es más el modo y el orden de su formulación. Las empresas externas de Auditoria Informática guardan sus Checklists, pero de poco sirven si el auditor no las utiliza adecuada y oportunamente. No debe olvidarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética.

El auditor deberá aplicar el Checklist de modo que el auditado responda clara y escuetamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario invitar a personal aquél a que exponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo.

Algunas de las preguntas de los Checklists empleadas para cada sector, deben ser repetidas. En efecto, bajo apariencia distinta, el auditor formulará preguntas equivalentes a las mismas o distintas personas y en las mismas fechas, o en fechas diferentes. De este modo, se podrán descubrir con mayor facilidad los puntos contradictorios; el auditor deberá analizar los matices de las respuestas y reelaborar preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad. El entrevistado no debe percibir un excesivo formalismo en las preguntas. El auditor, por su parte, tomará las notas imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia.

Los cuestionarios o Checklist responden fundamentalmente a dos tipos de "filosofía" de calificación o evaluación:

- **Checklist de Rango:**

Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo)
Se figuran posibles respuestas de los auditados. Las preguntas deben sucederse sin que parezcan encorsetadas ni clasificadas previamente. Basta con que el auditor lleve un pequeño guión. Por tanto la revisión de la Checklist no debe realizarse en presencia del auditado.

- **Trazas ó Huellas:**

Con frecuencia, el auditor informático debe verificar que los programas, tanto de los Sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Para ello se apoya en productos Software muy potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa.

Muy especialmente, estas "Trazas" se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en

absoluto el Sistema. Si la herramienta auditora produce incrementos apreciables de carga, se convendrá de antemano las fechas y horas más adecuadas para su empleo.

En lo referido al análisis del Sistema, los auditores informáticos emplean productos que comprueban los valores asignados por Técnica de Sistemas a cada uno de los parámetros variables de las Librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante. A modo de ejemplo, algunas instalaciones descompensan el número de iniciadores de trabajos de determinados entornos o toman criterios especialmente restrictivos o permisivos en la asignación de unidades de servicio para sus tipos carga. Estas actuaciones, en principio útiles, pueden resultar contraproducentes si se traspasan los límites.

No obstante la utilidad de las Trazas, ha de repetirse lo expuesto en la descripción de la auditoría informática de Sistemas: el auditor informático emplea preferentemente la amplia información que proporciona el propio Sistema: de manera que son los ficheros los ficheros de <Accounting> o <contabilidad>, en donde se encuentra la producción completa de aquél, y los <**Log** > de dicho Sistema, en donde se recogen las modificaciones de datos y se pormenoriza la actividad general.
Del mismo modo, el Sistema genera automáticamente exacta información sobre el tratamiento de errores de maquina central, periféricos.

La auditoria financiero-contable convencional emplea trazas con mucha frecuencia. Constituyen programas encaminados a verificar lo correcto de los cálculos de nóminas, primas.

- **Log:**

El log es un historial que informa que fue cambiando y cómo fue cambiando (información). Las bases de datos, por ejemplo, utilizan el log para asegurar las transacciones. Las transacciones son unidades atómicas de cambios dentro de una base de datos; todos los cambios se enmarcan dentro de una transacción, y todo lo

ejecutado por la Aplicación (grabar, modificar, borrar) dentro de esta, queda grabado en el log. La transacción tiene un inicio y un fin, cuando la transacción llega a su fin, se vuelca todo a la base de datos. Si en el medio de la transacción se cortó por x razón, lo que se hace es volver para atrás. El log te permite analizar cronológicamente que es lo que sucedió con la información que está en el Sistema o que existe dentro de la base de datos.

- **Software de Interrogación:**

Hasta hace ya algunos años se han utilizado productos software conocidos como paquetes de auditoria, capaces de generar programas para auditores escasamente calificados desde el punto de vista informático.

Más tarde, estos productos evolucionaron hacia la obtención de muestreos estadísticos que permitieran la obtención de consecuencias e hipótesis de la situación real de una instalación.

En la actualidad, los productos software especiales para la auditoria informática se orientan principalmente hacia lenguajes que permiten la interrogación de ficheros y bases de datos de la empresa auditada. Estos productos son utilizados solamente por los auditores externos, teniendo en cuenta que los internos disponen del software nativo propio de la instalación.

Del mismo modo, la proliferación de las redes locales y de la filosofía "Cliente-Servidor", han llevado a las firmas de software a desarrollar interfaces de transporte de datos entre computadoras personales y mainframe, de modo que el auditor informático copia en su propia computadora la información más relevante para su trabajo.

En la actualidad casi todos los usuarios finales poseen datos e información parcial generada por la organización informática de la Empresa. Efectivamente, conectados como terminales al "Host", almacenan los datos proporcionados por este, que son

tratados posteriormente en modo PC. El auditor se ve obligado (dependiendo del alcance de la auditoria) a recabar información de los mencionados usuarios finales, lo cual puede realizar con suma facilidad con los polivalentes productos descritos. Con todo, las opiniones más autorizadas indican que el trabajo de campo del auditor informático debe realizarse principalmente con los productos del cliente.

Finalmente, ha de indicarse la conveniencia de que el auditor confeccione personalmente determinadas partes del Informe. Para ello, resulta casi imprescindible una cierta soltura en el manejo de Procesadores de Texto, paquetes de Gráficos, Hojas de Cálculo.

1.7 Auditoria Informática de Sistemas Contables

La auditoria inicia como un órgano de control de algunas instituciones estatales y privadas con funciones estrictamente económico - financieras, y los casos inmediatos se encuentran en las peritaciones judiciales y las contrataciones de contables expertos por parte de Bancos Oficiales.

La función auditora debe ser absolutamente independiente; no tiene carácter ejecutivo. Queda a cargo de la empresa tomar las decisiones pertinentes. La auditoria contiene elementos de análisis, verificación y exposición de debilidades y disfunciones. Aunque pueden aparecer sugerencias y planes de acción para eliminar las disfunciones y debilidades referidas anteriormente; estas sugerencias plasmadas en el informe final reciben el nombre de recomendaciones.

La auditoria al sistema informático permite valorar la confiabilidad de la información procesada, el cumplimiento de lo establecido y el entorno de control en que se explotan las aplicaciones. Además del chequeo de los sistemas, el auditor somete al auditado a una serie de cuestionarios para tratar de explicar cómo ocurren los hechos. El auditor sólo puede emitir un juicio global o parcial basado en hechos y

situaciones incontrovertibles, careciendo de poder para modificar la situación analizada por él mismo.

1.8 Metodología de trabajo de Auditoria Informática(AI).

Para el desarrollo de la Auditoria Informática, el trabajo se organiza en las siguientes etapas:

- Alcance de la Auditoria Informática.
- Estudio inicial del entorno auditable.
- Determinación de los recursos necesarios para realizar la auditoria.
- Elaboración del plan y de los Programas de Trabajo.
- Actividades propiamente dichas de la auditoria.
- Confección y redacción del Informe Final.
- Redacción de la Carta de Introducción o Carta de Presentación del Informe final.

a) Definición del Alcance y Objetivos de la Auditoria Informática.

Objetivo

La Auditoria de Sistemas de Información no cambia la función de la auditoria, ni tampoco la condición y cualidades de auditor. Un elemento clave para planificar una auditoria de sistemas es traducir los objetivos básicos a objetivos específicos; ellos pueden enmarcarse en los siguientes puntos:

- Que se cumplan las políticas, normas y procedimientos que rigen esta actividad.
- Que se compruebe la seguridad de los recursos (personales, datos, equipamiento y software).
- Que se garantice, que la información que se procese sea confiable.
- Que se verifique el grado de privacidad del ambiente informático.
- Presentación de un informe para dar a conocer los resultados y recomendaciones.

- Los auditores de Sistemas de Información tienen las mismas responsabilidades y funciones del resto de los especialistas que participan en la auditoria, así como deben la misma observancia a las normas de auditorias y demás regulaciones establecidas.
- El alcance de la auditoria expresa los límites de la misma. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, las materias y las organizaciones a auditar.

A los efectos de acotar el trabajo, resulta muy beneficioso para ambas partes expresar las excepciones de alcance de la auditoria, es decir cuales materias, funciones u organizaciones no van a ser auditadas.

Tanto los alcances como las excepciones deben figurar al comienzo del Informe Final. Las personas que realizan la auditoria han de conocer con la mayor exactitud posible los objetivos a los que su tarea debe llegar. Deben comprender los deseos y pretensiones del cliente, de forma que las metas fijadas puedan ser cumplidas. Una vez definidos los objetivos (objetivos específicos), éstos se añadirán a los objetivos generales y comunes de toda auditoria informática: La operatividad de los Sistemas y los Controles Generales de Gestión Informática.

b) Estudio Inicial del Entorno Auditable

Para realizar dicho estudio ha de examinarse las funciones y actividades generales de la informática. Para su realización el auditor debe conocer lo siguiente:

Organización:

Para el equipo auditor, el conocimiento de quién ordena, quién diseña y quién ejecuta es fundamental. Para realizar esto un auditor deberá fijarse en:

1) Organigrama:

El organigrama expresa la estructura oficial de la organización a auditar.

Si se descubriera que existe un organigrama fáctico diferente al oficial, se pondrá de manifiesto tal circunstancia.

2) Departamentos:
Se entiende como departamento a los órganos que siguen inmediatamente a la Dirección. El equipo auditor describirá brevemente las funciones de cada uno de ellos.

3) Relaciones jerárquicas y funcionales entre órganos de la Organización:
El equipo auditor verificará si se cumplen las relaciones funcionales y jerárquicas previstas por el organigrama, o por el contrario detectará, por ejemplo, si algún empleado tiene dos jefes.
Las relaciones jerarquía implican la correspondiente subordinación. Las funcionales por el contrario, indican relaciones no estrictamente subordinables.

Flujos de Información:
Los flujos de información entre los grupos de una organización son necesarios para su eficiente gestión, siempre y cuando tales corrientes no distorsionen el propio organigrama. En ocasiones, las organizaciones crean espontáneamente canales alternativos de información, sin los cuales las funciones no podrían ejercerse con eficacia; estos canales alternativos se producen porque hay pequeños o grandes fallos en la estructura y en el organigrama que los representa. Otras veces, la aparición de flujos de información no previstos obedece a afinidades personales o simple comodidad. Estos flujos de información son indeseables y producen graves perturbaciones en la organización.

Número de puestos de trabajo.
El equipo auditor comprobará que los nombres de los puestos de trabajo del departamento correspondan a las funciones reales. Es frecuente que bajo nombres diferentes puestos de trabajo se realicen funciones idénticas, lo cual indica la existencia de funciones operativas redundantes.

Esta situación pone de manifiesto deficiencias estructurales: los auditores darán a conocer tal circunstancia y expresarán el número de puestos de trabajo verdaderamente diferentes.

Número de personas por puesto de trabajo.

Es un parámetro que los auditores informáticos deben considerar. La inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

Entorno operacional.

El equipo de auditoria informática debe poseer una adecuada referencia del entorno en el que va a desenvolverse. Este conocimiento previo se logra determinando, fundamentalmente, los siguientes extremos:

a) Se determina la ubicación geográfica del Centro de Proceso de Datos en la empresa. A continuación, se verificará la existencia de responsables en cada unos de ellos, así como el uso de los mismos estándares de trabajo.
b) Arquitectura y configuración de Hardware y Software:

Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas esta muy ligada a las políticas de seguridad lógica de la Empresa.

Los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.

c) Inventario de Hardware y Software:

El auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a hardware y la configuración de las PC, unidades de control local y remotas, y los periféricos de todo tipo.

El inventario de software debe contener todos los productos lógicos del Sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables.

d) Comunicación y redes de comunicación:
En el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones.
Igualmente, poseerán información de las redes locales de la Empresa.

Aplicaciones, bases de datos y ficheros
El estudio inicial que han de realizar los auditores se cierra y culmina con una idea general de los procesos informáticos realizados en la empresa auditada. Para ello deberán conocer lo siguiente:

- *Volumen, antigüedad y complejidad de las aplicaciones.*

- *Metodología del diseño*

Se clasificará globalmente la existencia total o parcial de metodología en el desarrollo de las aplicaciones. Si se han utilizados varias a lo largo del tiempo se pondrá de manifiesto.

- *Documentación*

La existencia de una adecuada documentación de las aplicaciones proporciona beneficios tangibles e inmediatos muy importantes.
La documentación de programas disminuye gravemente el mantenimiento de los mismos.
Cantidad y complejidad de bases de datos y ficheros.
El auditor recabará información de tamaño y características de las bases de Datos, clasificándolas en relación y jerarquías. Hallará un promedio de número de accesos a

ellas por hora o días. Esta operación se repetirá con los ficheros, así como la frecuencia de actualizaciones de los mismos.
Estos datos proporcionan una visión aceptable de las características de la carga informática.

Determinación de recursos necesarios para realizar la Auditoria Informática
Mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoria.

- **Recursos materiales**

Las herramientas software propias del equipo van a utilizarse igualmente en el sistema auditado, por lo que han de convenirse en lo posible las fechas y horas de uso entre el auditor y cliente.
Los recursos materiales del auditor son de dos tipos:

➢ Recursos materiales Software

Programas propios de la auditoria: Son muy potentes y flexibles. Habitualmente se añaden a las ejecuciones de los procesos del cliente para verificarlos.
Monitores: Se utilizan en función del grado de desarrollo observado en la actividad de Técnica de Sistemas del auditado y de la cantidad y calidad de los datos ya existentes.

➢ Recursos materiales Hardware

Los recursos hardware que el auditor necesita son proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en las computadoras del auditado.
Para lo cuál habrá de convenir, tiempo de maquina, espacio de disco, impresoras ocupadas.

- **Recursos Humanos**

La cantidad de recursos depende del volumen auditable. Las características y perfiles del personal seleccionado depende de la materia auditable.
Es igualmente reseñable que la auditoria en general suele ser ejercida por profesionales y por otras personas de probada experiencia multidisciplinaria.

Perfiles Profesionales de los auditores informáticos

Profesión	**Actividades y conocimientos deseables**
Informático General	Con experiencia amplia en ramas distintas. Deseable que su labor se haya desarrollado en Explotación y en Desarrollo de Proyectos. Conocedor de Sistemas.
Experto en Desarrollo de Proyectos	Amplia experiencia como responsable de proyectos. Experto analista. Conocedor de las metodologías de Desarrollo más importantes.
Técnico de Sistemas	Experto en Sistemas Operativos y Software Básico. Conocedor de los productos equivalentes en el mercado. Amplios conocimientos de Explotación.
Experto en Bases de Datos y Administración de las mismas.	Con experiencia en el mantenimiento de Bases de Datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación
Experto en Software de Comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Muy experto en Subsistemas de teleproceso.
Experto en Explotación y Gestión de CPD´S	Responsable del Centro de Cálculo. Amplia experiencia en Automatización de trabajos. Experto en relaciones humanas. Buenos conocimientos de los sistemas.
Técnico de Organización	Experto organizador y coordinador. Especialista en el análisis de flujos de información.

Técnico de evaluación de Costos	Economista con conocimiento de Informática. Gestión de costos.

Elaboración del Plan y de los programas de trabajo.

Una vez asignados los recursos, el responsable de la auditoria y sus colaboradores establecen un plan de trabajo. Decidido éste, se procede a la programación del mismo. El plan se elabora teniendo en cuenta, entre otros criterios, los siguientes:

a) La revisión se realizó por áreas generales y áreas específicas. En el primer caso, la elaboración es más compleja y costosa.
b) La auditoria es global o parcial. El volumen determina no solamente el número de auditores necesarios, sino las especialidades necesarias del personal.
c) En el plan no se consideran calendarios, porque se manejan recursos genéricos y no específicos. En el plan se establecen los recursos y esfuerzos globales que van a ser necesarios.
d) En el plan se establecen las prioridades de materias auditables, de acuerdo siempre con las prioridades del cliente.
e) El plan establece disponibilidad futura de los recursos durante la revisión.
f) El plan estructura las tareas a realizar por cada integrante del grupo.
g) En el plan se expresan todas las ayudas que el auditor ha de recibir del auditado.

Una vez elaborado el plan, se procede a la programación de actividades. Esta ha de ser lo suficientemente como para permitir modificaciones a lo largo del proyecto.

Actividades de la Auditoria Informática

Auditoria por temas generales o por áreas específicas:

La auditoria Informática general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos.
Cuando la auditoria se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se obtiene más rápidamente y con menor calidad.

Técnicas de Trabajo:
- Análisis de la información recabada del auditado.
- Análisis de la información propia.
- Cruzamiento de las informaciones anteriores.
- Entrevistas.
- Simulación.
- Muestreos.

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

Informe Final

La función de la auditoria se materializa exclusivamente por escrito. Por lo tanto la elaboración final es el exponente de su calidad.
Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.

Estructura del informe final:

El informe comienza con la fecha de comienzo de la auditoria y la fecha de redacción del mismo. Se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ostente.

Definición de objetivos y alcance de la auditoria.

Enumeración de temas considerados:

Antes de tratarlos con profundidad, se enumerarán lo más exhaustivamente posible todos los temas objeto de la auditoria.

Cuerpo expositivo:

Para cada tema, se seguirá el siguiente orden a saber:

a) Situación actual. Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real

b) Tendencias. Se tratarán de hallar parámetros que permitan establecer tendencias futuras.

c) Puntos débiles y amenazas.

d) Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoria informática.

e) Redacción posterior de la Carta de Introducción o Presentación.

- ***Modelo conceptual de la exposición del informe final:***

- El informe debe incluir solamente hechos importantes.

La inclusión de hechos poco relevantes o accesorios desvía la atención del lector.

- El Informe debe consolidar los hechos que se describen en el mismo.

El término de "hechos consolidados" adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados. La consolidación de los hechos debe satisfacer, al menos los siguientes criterios:

El hecho debe poder ser sometido a cambios.
Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.
No deben existir alternativas viables que superen al cambio propuesto.
La recomendación del auditor sobre el hecho debe mantener o mejorar las normas y estándares existentes en la instalación.
La aparición de un hecho en un informe de auditoria implica necesariamente la existencia de una debilidad que ha de ser corregida.
Flujo del hecho o debilidad:

1 – Hecho encontrado.

- Ha de ser relevante para el auditor y pera el cliente.
- Ha de ser exacto, y además convincente.
- No deben existir hechos repetidos.

2 – Consecuencias del hecho

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

3 – Repercusión del hecho

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

4 – Conclusión del hecho

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

5 – Recomendación del auditor informático

- Deberá entenderse por sí sola, por simple lectura.
- Deberá estar suficientemente soportada en el propio texto.
- Deberá ser concreta y exacta en el tiempo, para que pueda ser verificada su implementación.

La recomendación se redactará de forma que vaya dirigida expresamente a la persona o personas que puedan implementarla.

Carta de introducción o presentación del informe final:

La carta de introducción tiene especial importancia porque en ella ha de resumirse la auditoria realizada. Se destina exclusivamente al responsable máximo de la empresa, o a la persona concreta que encargo o contrato la auditoria.

Así como pueden existir tantas copias del informe final como solicite el cliente, la auditoria no hará copias de la citada carta de Introducción.

La carta de introducción poseerá los siguientes atributos:

Tendrá como máximo 4 folios.

Incluirá fecha, naturaleza, objetivos y alcance.

Cuantificará la importancia de las áreas analizadas.

Proporcionará una conclusión general, concretando las áreas de gran debilidad.

Presentará las debilidades en orden de importancia y gravedad.

En la carta de Introducción no se escribirán nunca recomendaciones.

CAPITULO II. DESARROLLO DE LA AUDITORIA INFORMATICA AL SISTEMA DE GESTION BAAN

2.1 Descripción del Sistema de Gestión BaaN, módulo Finanzas, implementado en la Empresa Pedro Sotto Alba.

BaaN (ERP) (Enterprise Resource Planning) Es un sistema empresarial de planeamiento de recurso diseñado para facilitar el control de las operaciones del negocio, de una manera eficiente que integran todos los aspectos funcionales de la empresa: Gestión comercial, gestión financiera, gestión de entradas / salidas, gestión de producción, control de almacenes etc. De esta forma el ahorro de tiempo y la minimización de errores es máximo, al no existir aplicaciones diferentes entre las cuales se transfieran datos, proceso que en muchos casos resulta imposible.

La Empresa Pedro Sotto Alba adquirió la licencia de operación de un Sistema Integrado de gestión que se encuentra en operaciones desde julio 1 del 2002. Este sistema es BaaN . Este es un software de origen Holandés.

Uno de los principales módulos es el de la gestión en la satisfacción de las necesidades de administración financiera BaaN_Finanzas. Este módulo está compuesto por:

- Contabilidad de clientes
- Contabilidad de proveedores
- Sistema de presupuestos
- Gestión de tesorería
- Asignación de costos
- Informes financieros
- Activos fijos
- Contabilidad general

BaaN _Finanzas proporciona a la entidad flexibles facilidades de informes financieros e información actualizada necesaria para gestionar las operaciones diarias. Además, la Empresa podrá beneficiarse con la posibilidad de operar en múltiples idiomas y monedas y un soporte de BaaN _Finanzas para gestionar múltiples operaciones de venta. Asimismo, podrá confeccionar informes financieros de acuerdos a las normativas y los diferentes tipos de monedas en la que opera la Empresa. El sistema es capaz de consolidar y fusionar toda la información financiera de operaciones individuales e integrar los datos en múltiples niveles de la Empresa. Se beneficiará además de una completa transparencia de los datos financieros a todos los niveles de la organización gracias a la capacidad de profundización del sistema.

BaaN_Finanzas, permite a la empresa procesar y obtener información financiera en tiempo real, con lo que la administración se lleva a cabo de forma proactiva, ayudando a la toma de decisiones más apropiadas, las acciones pueden ejecutarse puntualmente y se simplifican los procesos empresariales. BaaN _Finanzas actualiza automáticamente todos los niveles de las transacciones una vez introducida por lo que el sistema genera en todo momento la información actualizada y posibilita efectuar transacciones por lotes en el caso de que los datos no estén sujetos a esta disponibilidad inmediata.

Los procedimientos y necesidades de registro de transacciones financieras difieren de un mercado y país a otro y la aplicación BaaN_Finanzas, permite a la Empresa gestionar fácilmente dichas diferencias. Por ejemplo, se adapta a los métodos de diversos países para la gestión del impuesto del valor añadido. Las funciones estándar incorporadas en el sistema permiten acomodarse a la legislación local en lo que se refiere a los métodos de pago en Canadá y la mayoría de países de Europa occidental. Asimismo, BaaN _Finanzas contempla métodos de pagos como la orden bancaria, la letra de cambio y el pago electrónico. Los múltiples calendarios del sistema pueden gestionar hasta 99 períodos. La función de calendario proporciona la

capacidad de llevar a cabo transacciones diarias en calendario de ejercicio fiscal y procesar los datos por año natural a efectos tributarios.
Para perfeccionar los procesos financieros de la empresa y como ayuda en la gestión de múltiples plantas, operaciones y organizaciones de venta, BaaN _Finanzas ofrece la capacidad de consultar la información de varias entidades financieras en una sola vez. Por ejemplo, es posible gestionar la información a nivel de grupo en los módulos Contabilidad general, Contabilidad de proveedores y Contabilidad de clientes y generar transacciones de entrada automáticamente.

Con BaaN_Finanzas, una empresa puede registrar centralmente todos los pagos de un grupo de empresas y consultar los saldos totales de cuentas contables, clientes o proveedores específicos bien agrupadamente como individualmente. Además, pueden consultarse informes de la contabilidad general, de la contabilidad proveedores y de la contabilidad de clientes tanto a nivel de la entidad como de grupo. La estructura flexible de las cuentas de BaaN _Finanzas permiten acceder fácilmente a información a nivel de resumen, y es posible configurar la contabilidad general y la de clientes para que tengan un nivel superior, lo cual facilita la gestión de los compromisos financieros y del crédito.

BaaN _Finanzas ofrece así mismo funciones de banco electrónico. Gracias a esta posibilidad, la Empresa puede efectuar los pagos simplemente generando un archivo y enviándolo luego al banco. Los cobros procedentes del banco se concilian automáticamente con los asientos pendientes, lo que elimina el tedioso trabajo de introducción de datos.

Para el banco electrónico, el sistema emplea la función de procesamiento de transacciones para las transacciones bancarias introducidas manualmente. Éstas se imprimen entonces en extractos bancarios. Dado que algunos bancos proporcionan extractos bancarios electrónicos, BaaN _Finanzas los convierte y los importa. Los pagos compuestos que recibe de un cliente la Empresa por medios electrónicos

pueden estar acompañados por un mensaje de aviso de remesa que contiene información acerca del pago compuesto.

Así mismo, BaaN _Finanzas convierte los extractos bancarios y cualquier mensaje de aviso de remesa adjunto y los concilia con las facturas de venta y de compra. La información necesaria se procesa entonces en cuentas financieras. Estas funciones electrónicas pueden realizarse para los siguientes tipos de transacciones: transacciones de clientes, de proveedores, conciliación de pagos de clientes y de proveedores.

- **Módulo de Contabilidad de Cliente.**

El módulo Contabilidad de clientes de BaaN _Finanzas ofrece la posibilidad de ejercer un control total sobre las cuentas de los clientes y proporciona la información necesaria para tomar las decisiones más certeras y oportunas. Este módulo supervisa, gestiona y procesa facturas de venta y, al poder detectar las facturas vencidas, el sistema asegura el cobro de los conceptos pendientes de pago. Además, la Empresa puede beneficiarse del soporte en línea de la gestión de crédito. De esta forma, durante una reclamación telefónica, por ejemplo, es posible registrar los motivos del impago e indicar la acción de seguimiento apropiada. Generando reclamaciones fácilmente.

El sistema mantiene un programa de cobros, que permite a la empresa poder indicar a los clientes los importes pagados o pendientes de pago correspondientes a una factura. Es posible además registrar clientes dudosos en los casos que parece improbable que llegue a efectuarse el cobro de una factura. Toda la información correspondiente a las cuentas a cobrar se incluye automáticamente en previsiones de tesorería e informes de clientes, y es posible vincular cada cliente a un grupo de clientes con sus propias cuentas y dimensiones. Por otra parte, pueden utilizarse facturas ya para asegurar que no se inicia el procedimiento de una orden de venta hasta no haber recibido un pago a cuenta. La función de facturas pro-forma de

BaaN_Finanzas está integrada también en las aplicaciones BaaN_Proyecto y BaaN_Distribución.

- **Simplificación de los pagos mediante el módulo Contabilidad de proveedores.**

El módulo Contabilidad de proveedores de BaaN Finanzas ofrece avanzadas posibilidades de gestión de las cuentas de proveedores de la Empresa. Como saben la mayoría de directores administrativos, uno de los principales aspectos de la contabilidad de clientes es el registro y conciliación de las facturas con las órdenes de venta y las aprobaciones necesarias para ello. *Gracias a BaaN*_Finanzas, es posible definir un plan de autorizaciones para las facturas recibidas, con el cual el responsable o departamento puede autorizar la factura electrónicamente antes de efectuar el registro y el pago.

Asimismo, existe la posibilidad de recibir facturas electrónicamente y procesarlas de forma similar que las facturas registradas manualmente. Por otra parte, las órdenes de compra y las facturas se concilian automáticamente para ahorrar tiempo y trabajo. Definiéndose además tolerancias a efectos de la conciliación automática y programas de pago que indiquen en qué momento una factura ha vencido total o parcialmente.

La información que ofrece BaaN _Finanzas sobre las facturas de compra pendientes de pago, proporciona a la empresa detalles sobre las facturas contabilizadas, como la fecha de descuento y la de vencimiento, posibilitando revisar y modificar la información según sea necesario. Asimismo, pueden liquidarse diferencias de pago y especificar si deben o no calcularse beneficios por cambio de divisa en el momento de revalorizar los pagos pendientes.

Además, no resulta difícil supervisar las facturas de los proveedores, teniendo en cuenta que en el archivo de esta información es posible bloquear las órdenes o

pagos a un determinado proveedor y una vez pagadas totalmente las facturas, pueden eliminarse del sistema o archivarse.

- **Módulo Presupuestos.**

Para cualquier Empresa, la confección de presupuestos detallados es fundamental en la proyección financiera . A fin de otorgar a la Empresa la capacidad de gestionar presupuestos en cada nivel de la misma, el módulo Presupuestos de BaaN _Finanzas utiliza datos de todo el sistema de gestión financiera. El sistema permite crear un número ilimitado de presupuestos anuales, lo que significa que la Empresa puede mantener un presupuesto original, uno corregido, otro simulado y una estimación actual. Además, puede calcular automáticamente la última estimación mediante un rango de períodos actuales. Las cifras reales se emplean para calcular nuevos presupuestos, y es posible distribuir presupuestos anuales a lo largo de varios ejercicios fiscales utilizando porcentajes y factores.

Ser generado, pueden crearse múltiples presupuestos y analizarlos en sentidos "ascendente" y "descendente". El método ascendente registra los presupuestos en el nivel inferior y genera subtotales y totales automáticamente, mientras que el método descendente los registra en niveles superiores; ejemplo: para un departamento. Los presupuestos de nivel superior se asignan a libros mayores individuales.

- **Módulo de Gestión de tesorería.**

Una previsión eficaz de la tesorería es fundamental para asignar y controlar los costos de cualquier empresa. El módulo Gestión de tesorería de BaaN _Finanzas permite beneficiarse de un versátil sistema de gestión de tesorería además de importantes funciones de los diferentes tipos de monedas. Es posible registrar automáticamente la información de tesorería a nivel de grupo o de Empresa individual generando parcialmente las previsiones de tesorería se generan fácilmente. Para disponer de fondos rápidamente, el sistema incorpora asimismo una

función de tele banco tanto para los cobros como para los pagos. Además, es posible imprimir facturas proforma en función de un programa de cobros anticipados y vincularlas entonces a los cobros anticipados correspondientes al importe apropiado antes de entregar los artículos vendidos.

- **Módulo de Asignación de costos.**

A medida que se reducen los ciclos vitales de los productos y los mercados son cada vez más competitivos, la asignación de costos precisa se ha convertido en una cuestión fundamental para la rentabilidad de cualquier empresa. El módulo Asignación de costos de BaaN _Finanzas proporciona a la empresa la información precisa sobre los costos, además de instaurar un sólido control de los mismos.

Este sistema permite aumentar la precisión de la asignación de costos debido a que éstos se derivan de los datos financieros y demás datos extraídos de otras aplicaciones BaaN. Este método proporciona a los directores de la Empresa una mayor capacidad de conocimiento de las actividades de la organización que sirven parea determinar los costos por objeto de costo.

- **Informes financieros.**

Debido a que las estructuras organizativas y financieras experimentan frecuentes cambios en las empresas modernas, la mayoría de la empresas precisan que su sistema de informes financieros sea flexible. El módulo Informes financieros de BaaN _Finanzas proporciona a la Empresa información detallada y listados de datos financieros. Posibilita las consolidaciones multinivel entre distintos sistemas contables y existe además una potente función para la eliminación. La información presentada en los informes puede emplearse para definir un número ilimitado de ratios y mantenerlos entonces como registros históricos.

- **Módulo de Activos fijos**

El módulo Activos fijos de BaaN _Finanzas permite llevar un control preciso de los activos de una empresa. Los métodos de amortización del sistema pueden definirse libremente, y es posible calcular los costos de amortización tantas veces como sea necesario. Hay diversos métodos que están disponibles para calcular una amortización: según el valor inicial de venta, el valor amortizado a principio de un ejercicio fiscal o una combinación de ambos. Es posible además calcular la amortización según las necesidades locales de países diferentes y debido a que el módulo Activos fijos está completamente integrado con el módulo Contabilidad general, toda la información como el beneficio o pérdida contable, se contabilizan automáticamente en éste. El sistema incluye también funciones de simulación que pueden emplearse para conocer las consecuencias de futuras inversiones.

- **Módulo Contabilidad General**

El módulo Contabilidad general de BaaN _Finanzas proporciona a la empresa la flexibilidad necesaria para establecer y redefinir cuentas contables que se adapten a los cambios. En él se mantienen tanto importes como información estadística. Las pantallas de la interfaz del usuario pueden personalizarse, siendo posible consultar y listar la información en cualquier formato deseado. El módulo soporta cuentas de subnivel, y cada una de éstas se enlaza a una cuenta contable superior, proporcionando una forma versátil de obtener información a todos los niveles.

En un gran número de países, el libro mayor debe contener muchos datos, pero los directores administrativos deben procurar también que sea posible acceder a información detallada sobre importes específicos. Para ello, BaaN _Finanzas proporciona cinco dimensiones que pueden ser definidas libremente a fin de desglosar los datos financieros en componentes como departamentos, centros de costo, unidades de negocio, grupos de producto y regiones de venta. Permitiendo crear una estructura organizativa completa entre y dentro de las cinco dimensiones.

El procesamiento central del módulo Contabilidad general permite actualizar las transacciones de la forma más apropiada a la Empresa: en tiempo real, al finalizar una sesión de entrada de datos o mediante actualizaciones periódicas por lotes. Además, es posible utilizar simultáneamente múltiples tipos de transacciones a fin de satisfacer las necesidades específicas de los diversos departamentos de la organización.

Las transacciones automáticas de BaaN _Finanzas permiten asimismo reducir el trabajo de introducción de datos, ya que es posible redefinir los datos de transacciones y ordenar que se efectúen en una sola operación. Las transacciones distribuidas a lo largo del tiempo únicamente necesitan introducirse una sola vez, tras lo cual se contabilizan al período apropiado. Asimismo, es posible simplificar las transacciones entre Empresas generándolas automáticamente y beneficiarse a partir de las posibilidades de las entradas recursivas e inversas y de las transacciones especiales preparadas para registrar notas de abono. Además, es posible procesar facturas de compra que se originan en sistemas informáticos distintos de BaaN Finanzas.

El motor de base de datos que soporta este sistema es Oracle, un potente gestor que constituye un valor agregado del sistema. También facilita la interacción con reporteadores como Crystal, que son utilizados para publicar información de forma interactiva y en tiempo real a los directores, supervisores de plantas, administradores de proyectos, etc. Lo reportes creados satisfacen pedidos personalizados de los clientes y facilitan el seguimiento y análisis de los costos, importaciones, etc.
Contamos con un excelente soporte técnico desde BaaN– Venezuela aunque el mismo no se limita a esta sucursal. El soporte es global y nuestros especialistas del Dpto. de Tecnología de la información tienen acceso a la base de conocimientos que está disponible desde el sitio en Internet de SSA – Global para todos sus clientes.

Por otra parte, la operación del sistema requiere de habilidades que son adquiridas con un entrenamiento adecuado. Por ello los entrenamientos y los nuevos procesos

que se desean implementar son realizados en un servidor de pruebas antes de hacerlo en el servidor de producción. Ello evita errores y fallas que pueden ser introducidas por los usuarios. El acceso al menú de opciones es similar al ofrecido por el explorador de Windows (ver Anexo 2).

Los módulos constan de múltiples opciones para consultas y reportes. Los mismos están disponibles para todos los usuarios del sistema, pero las opciones de adiciones, modificaciones y cálculos están restringidas por accesos que han sido autorizados por los jefes de los departamentos correspondientes. Una lista de los accesos por usuarios está disponible para consultas y a efecto de control interno.

2.2 Resultados de la Auditoria Realizada.

Sobre el ejercicio económico del año 2005, se realiza una revisión de los Controles Generales del Sistema Informático como soporte a la Auditoria Informática (AI), incluyendo principalmente los siguientes aspectos:
Nota: Se actualizará el entendimiento para los 10 perfiles de Controles Generales y se aplicarán pruebas para 7 de ellos (**marcados en negrita**):

Perfiles a Considerar
A) Estrategia y Planeación de Recursos de Información
B) Operaciones de los Sistemas de Información
C) Relaciones con los Proveedores Externos
D) Seguridad de la Información
E) Planeación de la Continuidad del Negocio
F) Implementación y Mantenimiento de los Sistemas de Aplicación
G) Implementación y Soporte de la Base de Datos
H) Soporte de la Red
I) Soporte del Software de los Sistemas
J) Soporte del Hardware

Se realizaron entrevistas con el personal involucrado en estas áreas para comprender los controles implementados y su supervisión.

El tiempo requerido para hacer entrevistas con el personal de sistemas involucrado con los puntos antes mencionados, fue de una hora como máximo para cada uno; el tiempo restante es dedicado a documentar y elaborar papeles de trabajo, y solo se volverá a recurrir al personal en caso de dudas y aclaraciones.

Para poder complementar nuestra revisión, solicitamos copias fotostáticas de la siguiente documentación a reserva de ser revisada de la cual es posible que algunos puntos no apliquen:

Área / Documento
Conocimiento del cliente:
Organigrama vigente del área de Sistemas
Diagrama de distribución de equipo de cómputo (servidores y tcomms)
Perfiles de puestos del personal del área de Sistemas
Inventario de software y hardware
A) Estrategia y Planeación de Recursos de Información
Planeaciones y Proyectos (Nuevos y en vías de desarrollo)
B) Operaciones de los Sistemas de Información
Políticas y procedimientos (portada e índice)
Procedimientos de respaldo (portada e índice)
Bitácoras de procesos, errores, respaldos y pruebas de respaldos (la mas reciente)
Inventario de cintas de respaldo (último)
Contrato vigente con el Banco de caja de seguridad
Relación de cintas offsite (última) y registro de movimientos de cintas offsite
C) Relaciones con los Proveedores Externos
Contratos vigentes con Proveedores Externos
D) Seguridad de la información

Políticas y procedimientos (portada e índice)

Listado de empleados vigentes

Solicitudes de altas, bajas y/o modificaciones a las capacidades de acceso

Diagramas de seguridad

Notificación de confidencialidad a los usuarios

Registros de entrada del SITE (el mas reciente)

E) Planeación de la Continuidad del Negocio

Plan de Continuidad del Negocio

F) Implementación y Mantenimiento de los Sistemas de Aplicación

Estándares de desarrollo (portada e índice)

Manuales para usuarios, Manuales técnicos y Manuales de Programador (portada e índice)

Licencias de software (1 de cada marca)

Documentación de los programas

G) Implementación y Soporte de la Base de Datos

Procedimientos de mantenimiento de las bases de datos

H) Soporte de la Red

Diagrama de red

Software instalado en la red

Bitácoras de Operación, Errores y Respaldos (portada e índice)

I) Soporte del Software de los Sistemas

Avances de desarrollo (los mas recientes)

Planes de capacitación (los mas recientes)

Solicitudes de usuarios (los mas recientes)

Procedimientos de Prueba y liberación de desarrollos

Prioridades de desarrollo

J) Soporte del Hardware

Bitácoras de Mantenimiento

Calendario de Revisiones

Contrato con el proveedor externo

Esta auditoria se desarrolla con el personal de DELOITTE.ERS (Enterprise Risk Services), con los auditores financieros de la empresa Pedro Sotto Alba para un periodo comprendido del 1 enero al 31 de Diciembre 2005.

El equipo que realiza la auditoría debe determinar la confiabilidad de los ambientes de procesamiento de la información financiera en los ciclos de negocios relacionados, así como la identificación de las áreas de oportunidad que necesitan ser consideradas como apoyo a la auditoria financiera.

Actividades de Auditoria

El trabajo se iniciará con la revisión de las condiciones generales del negocio, así como del riesgo de auditoria basándonos en las entrevistas sostenidas con el personal ejecutivo de sistemas de la Empresa, la comprensión general de los sistemas y tecnología de computación y los antecedentes de auditorias pasadas.

Se continuará con el plan de rotación que se tiene definido para la evaluación de los controles generales del computador (segundo año de revisión), a través de la definición y aplicación de pruebas sobre los controles implementados, lo cual implica revisar los perfiles que no han sido considerados en años anteriores, de acuerdo a como lo indica nuestra metodología **(4 perfiles)**, mas adelante se puede ver el detalle.

Además de realizar la revisión de los perfiles, utilizando la herramienta Checklist, se realizan pruebas sobre el servidor donde está instalado el sistema BaaN, verificándose la configuración general de dicho sistema.

Alcance del trabajo

Controles Generales del Sistema Informático: Son los controles que corresponden al área de sistemas de lMoa Nickel, S.A., así como a la infraestructura que soporta el correcto procesamiento de las operaciones de la Empresa

El alcance de nuestra revisión contempla lo diez controles generales de la computadora de los siguientes perfiles:

1. Planeación y estratégica de los recursos de información
2. Operaciones de los sistemas de información
3. Relaciones con proveedores externos
4. **Seguridad en la información.**
5. Planeación de la continuidad del negocio
6. **Mantenimiento e implantación de los sistemas de aplicación**
7. **Soporte e implementación a la base de datos**
8. Soporte a la red
9. **Soporte al software de sistemas**
10. Soporte al hardware

Como anteriormente se comentaba, se actualizará la información para los 10 perfiles de controles generales de la computadora, además de que se aplicarán pruebas para 4 de ellos (**marcados en negrita**):

Evaluación de los *Controles Generales del Sistema Informático* como Soporte a Auditoria Financiera al período que cierra el 31 de Diciembre del 2005.

Objetivos de la revisión.

Como parte integral de la auditoria de estado financieros para saber si el ambiente de control de la empresa conduce generalmente a un procesamiento de información financiera confiable y aun control interno efectivo, es necesario realizar una evaluación del ambiente de procesamiento de la información. Este trabajo debe verse dentro del contexto de la Auditoria Informática.

Se realizó una evaluación del control interno del área de sistemas de acuerdo con el plan de rotación que se tiene para la auditoria informatica y concluir si el ambiente de procesamiento soporta la generación de información financiera contable.

• Recomendar a la auditoria financiera una estrategia de confianza en controles de acuerdo con nuestra evaluación.
• Proporcionara recomendaciones de valor agregado de la Empresa , con el objetivo que le permita fortalecer el control interno de la organización.

COMENTARIOS GENERALES

Categorías de Riesgos:

• **ALTO (A):** Representa un riesgo latente de alguna pérdida inmediata en las finanzas o en la integridad de la información. Deberá ser atendido lo antes posible.

• **MEDIO (M):** Representa un riesgo potencial en la pérdida de la información financiera o en la integridad de los datos. Deberá ser atendido durante los siguientes 30-90 días.

• **BAJO (B):** Representa un riesgo mínimo en la pérdida de la información financiera o en la integridad de los datos. Deberá ser atendido cuando sea posible y para ello podrá intervenir personal del área de tecnología de información de la empresa.

Esfuerzo para Corregir:

• **ALTO (A):** Se necesita un esfuerzo inmediato para eliminar o mitigar este posible riesgo. Se puede requerir más de un mes para poder implantar la solución.

• **MEDIO (M):** Se requiere un esfuerzo regular para eliminar o mitigar el riesgo. La implantación de la solución puede tomar de uno a treinta días.

• **BAJO (B):** La solución podrá implantarse de manera inmediata.

Los resultados de la auditoria realizada sobre los *Controles Generales del Sistema Informático fue realzada el 25 de noviembre del 2005 lo cuales fueron ejecutada por las siguientes personas.*

Personal presente en la auditoria.

Martha Montes de Oca Corrales (Jefe Departamento IT de la Empresa Pedro Sotto Alba-PSA)

Héctor Salermo (Infraestructura de Redes y Servidores- PSA)

Yanisa Peña (Analista de Sistemas- PSA)

Marcos Antonio Cervantes Díaz (Consultor de Deloitte)

1.- Plan de Recuperación en Caso de Desastres (DRP).

<table>
<tr><th>Observación</th><th colspan="2">Comentarios del Cliente</th></tr>
<tr><td>Hay oportunidades relacionadas con el contenido del DRP; debido a que este se integra de una lista de situaciones que pueden afectar el funcionamiento normal de los sistemas de información y las actividades seguir en caso de una contingencia.
Plan actual que tiene la empresa:
• Infraestructura de las áreas / procesos críticos
• Riesgos que amenazan el desempeño de los sistemas de información, medidas preventivas y estrategias de la recuperación, deberes y responsabilidades
Existen puntos que sería recomendable implementar:
• Impacto en caso de que los riesgos se materialicen
Pasos para declarar una contingencia.
• Plan de pruebas parciales e integrales</td><td colspan="2">De acuerdo con la observación, se intentará corregir, sin embargo esto implica una gran inversión de horas hombre.</td></tr>
<tr><td rowspan="2"></td><td>Riesgo</td><td>Esfuerzo para Corregir</td></tr>
<tr><td>MEDIO (M)</td><td>ALTO (A)</td></tr>
</table>

2.- Seguridad Física del Cuarto del Servidor

<table>
<tr><th>Observación</th><th colspan="2">Comentarios del Cliente</th></tr>
<tr><td rowspan="2">Hay oportunidades relacionadas con los controles de acceso físico y control del ambiente en los lugares dónde se tiene instalado el equipo crítico (los servidores e infraestructura de la telecomunicación), cuarto del servidor e IDF en la planta. Las recomendaciones principales se detallan a continuación:
• Considerar la posibilidad de instalar un detector de incendios automático y un sistema de supresión conectado a las alarmas
•Sistema de circuito cerrado integrado por varias cámaras instaladas dentro y fuera del sitio principal y los sitios alternos, así como un software de grabación y terminales de monitoreo en los puestos de vigilancia.</td><td colspan="2">Se reforzará la seguridad de la puerta de acceso al sitio, se investigará una mejor opción para la supresión de incendios, ya que el gas Halon daña la capa de ozono. Se han iniciado investigaciones referentes a la supresión de incendios, sin embargo la solución presentada por los proveedores no ha sido satisfactoria al introducir riesgos adicionales a la operación normal del sistema.</td></tr>
<tr><td>Riesgo</td><td>Esfuerzo para Corregir</td></tr>
<tr><td></td><td>MEDIO(M)</td><td>ALTO (A)</td></tr>
</table>

3.- Mantenimiento Preventivo del Equipo de Cómputo

<table>
<tr><th>Observación</th><th colspan="2">Comentarios del Cliente</th></tr>
<tr><td rowspan="3">No se cuenta con un programa que especifique las fechas en las que se tiene definido dar mantenimiento preventivo al equipo de cómputo (servidores), además de que no se cuenta con el soporte documental de los servicios de mantenimiento preventivo y correctivo que se han realizado sobre los mismos, con la finalidad de tener el detalle y resultados del servicio.</td><td colspan="2">La Empresa realiza mantenimiento preventivo de oportunidad (cuando la operación permite suspender los servicios). Se trabajará en documentar los resultados de los mantenimientos. Se realizó un mantenimiento del servidor principal de BaaN en marzo y se realizará uno nuevamente en diciembre debido a la implementación del nuevo sistema de respaldos en este tipo de servidores.</td></tr>
<tr><td>Riesgo</td><td>Esfuerzo para Corregir</td></tr>
<tr><td>BAJO (B)</td><td>MEDIO (M)</td></tr>
</table>

4.- Inventario de Software Instalado.

Observación	Comentarios del Cliente
Durante el 2005 la Empresa no ha realizado una revisión detallada del software instalado en los equipos de la Empresa, con el cual se identifique software instalado que no sea propiedad de la Empresa y el cual no este considerado dentro de las herramientas de los usuarios para el desempeño de sus funciones cotidianas. El riesgo de esta observación se minimiza debido a que la mayoría de los equipos actualmente cuentan con sistemas	Se programará para el 2006 un inventario de software en máquinas Windows´ 95

operativos Windows 2000 o Windows XP en los cuales los usuarios no tienen privilegios suficientes para instalar software en los equipos.		
	Riesgo	Esfuerzo para Corregir
	BAJO (B)	MEDIO (M)

5.- Administración de Cuentas de Acceso a la Red.

Observación	**Comentarios del Cliente**	
Se identificaron algunas áreas de oportunidad dentro la administración de la cuentas de acceso a la red y la aplicación algunas políticas de seguridad de la Empresa. Existen 9 usuarios que no han ingresado a la red en mas de 3 meses y a los cuales no se les ha deshabilitado la clave de acceso. La mayor parte de estos corresponde a usuarios que se conectan al dominio esporádicamente por la naturaleza de sus funciones, a excepción del usuario “afernan” quien cubría un permiso vacacional y “agmillet”. La clave de acceso de estos usuarios ya expiró a la fecha de nuestra revisión, lo cual mitiga el riesgo, sin embargo, se sugiere realizar una revisión de los mismos para evaluar si es necesario darlos de baja de la red, o en su defecto bloquearlos. • Se identificaron 12 usuarios que nunca se han registrado haciendo operaciones en la red. De estos, 9 corresponden a usuarios de Halifax que se crearon y nunca se utilizaron. Los otros tres solamente han utilizado los servicios de Internet.	Se incluirán estos puntos dentro del monitoreo constante que realiza la Empresa. Para el usuario agmillet se decidido eliminar o a bloquear al usuario. Se verificó contra un correo para el jefe del usuario. Para “efernan” se revisará también. Para los 9 usuarios de Halifax se tomará una acción correctiva.	
	Riesgo	**Esfuerzo para Corregir**
	BAJO (B)	**BAJO (B)**

6.- Definición de Perfiles para el Área de Tecnología de la Información

<table>
<tr><th>Observación</th><th colspan="2">Comentarios del Cliente</th></tr>
<tr><td rowspan="2">La Subdirección Recursos Humanos no cuenta con perfiles definidos para los puestos del área de sistemas de información, que especifiquen los requisitos que deben cubrir los prospectos durante el proceso de selección de personal para dichos puestos, como niveles de estudios, experiencia laboral y resultados de exámenes psicométricos, entre otros. Actualmente el departamento de TI mantiene descripciones de puestos y responsabilidades actualizados y en caso de requerir personal para cubrir una vacante se le especifica a RH el perfil que debe tener el aspirante a ocupar el puesto.</td><td colspan="2">De acuerdo con la observación se trabajará en desarrollar los perfiles de los puestos para el área de TI.</td></tr>
<tr><td>Riesgo</td><td>Esfuerzo para Corregir</td></tr>
<tr><td></td><td>BAJO (B)</td><td>BAJO (B)</td></tr>
</table>

7.- Documentación de Pruebas Realizadas

Observación	**Comentarios del Cliente**	
La Empresa no mantienen documentación referente a las pruebas realizadas para la implementación de nuevos sistemas, aplicaciones o a la instalación de software de red y de sistemas. Derivado de lo anterior no nos fue posible corroborar que el diseño y la realización de las pruebas fueran adecuados y que el resultado de las mismas fuera debidamente revisado por la gerencia para su posterior aplicación en ambientes productivos.	Se realiza para los sistemas y servidores principales, sin embargo, esta labor se hará extensiva a todas las implementaciones.	
	Riesgo	**Esfuerzo para Corregir**
	BAJO (B)	BAJO (B)

2.4 Ejercicio de comprobación del Ciclo de Seguridad de Derechos a los Usuarios del Módulo BaaN Finanzas.

Es una auditoria de Seguridad Informática que tiene como misión revisar tanto la seguridad física del Centro de Proceso de Datos en su sentido más amplio, como la seguridad lógica de datos, derechos de los usuarios asignado por el administrador del sistema BaaN en los procesos y funciones informáticas más importantes, usando la Software CRMR (Computer Resource Manager Review). Que se usa para realizar la evaluación de la gestión de recursos informáticos, para una evaluación de eficiencia.

Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN_ Finanzas

El objetivo de esta auditoria de seguridad es revisar la situación y las cuotas de eficiencia de la misma en los órganos más importantes de la estructura informática.

Para ello, se fijan los supuestos de partida:

El área auditada es la Seguridad.

El área a auditar se divide en: *Segmentos*.

Los segmentos se dividen en: *Secciones*.

Las secciones se dividen en: *Subsecciones*.

De este modo la auditoria se realizara en 3 niveles.

Los segmentos a auditar, son:

Segmento 1: Seguridad de cumplimiento de normas y estándares.

Segmento 2: Seguridad de Sistema Operativo.

Segmento 3: Seguridad de Software en BaaN_Finanzas.

Segmento 4: Seguridad de Comunicaciones.

Segmento 5: Seguridad de Base de Datos.

Segmento 6: Seguridad de Proceso.

Segmento 7: Seguridad de Aplicaciones.

Segmento 8: Seguridad Física.

Se darán los resultados globales de todos los segmentos y se realizará un tratamiento exhaustivo del Segmento 8, a nivel de sección y subsección.

Conceptualmente la auditoria informática en general y la de Seguridad en particular, ha de desarrollarse en seis fases bien diferenciadas:

Fase 0. Causas de la realización de **Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN_Finanzas**

Fase 1. Estrategia y logística de **Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN _Finanzas**

Fase 2. Ponderación de sectores **Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN_Finanzas**

Fase 3. Operativa del **Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN _Finanzas**

Fase 4. Cálculos y resultados del **Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN _Finanzas** .

Fase 5. Confección del informe del **Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN _Finanzas** .

A su vez, las actividades auditoras se realizan en el orden siguiente:

- Comienzo del proyecto de Auditoría Informática.
- Asignación del equipo auditor.
- Asignación del equipo interlocutor del cliente.
- Llenado de formularios globales y parciales por parte del cliente.
- Asignación de pesos técnicos por parte del equipo auditor.
- Asignación de pesos políticos por parte del cliente.
- Asignación de pesos finales a segmentos y secciones.
- Preparación y confirmación de entrevistas.
- Entrevistas, confrontaciones y análisis y repaso de documentación.
- Calculo y ponderación de subsecciones, secciones y segmentos.
- Identificación de áreas mejorables.
- Elección de las áreas de actuación prioritaria.
- **Preparación de recomendaciones y borrador de informe**
- Discusión de borrador con cliente.
- Entrega del informe.

Causas de realización de una Auditoría de Seguridad

Esta constituye la FASE 0 de la auditoría y el orden 0 de actividades de la misma. El equipo auditor debe conocer las razones por las cuales el cliente desea realizar el **Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN_Finanzas.**

Puede haber muchas causas: Reglas internas del cliente, incrementos no previstos de costos, obligaciones legales, situación de ineficiencia global notoria.

De esta manera el auditor conocerá el entorno inicial. Así, el equipo auditor elaborará el Plan de Trabajo.

Estrategia y logística del Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN _Finanzas

Constituye la FASE 1 Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN _Finanzas se desarrolla en las actividades 1, 2 y 3:

Fase 1. Estrategia y logística del Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN _Finanzas Designación del equipo auditor.

Asignación de interlocutores, validadores y decisores del cliente.
Cumplimentación de un formulario general por parte del cliente, para la realización del estudio inicial. Con las razones por las cuales se realiza la auditoría (Fase 0), el equipo auditor diseña el proyecto Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN _Finanzas con arreglo a una estrategia definida en función del volumen y complejidad del trabajo a realizado, que constituye la Fase 1 del punto anterior.

Para desarrollar la estrategia, el equipo auditor necesita recursos materiales y humanos. La adecuación de estos se realiza mediante un desarrollo logístico, en el que los mismos deben ser determinados con exactitud. La cantidad, calidad, coordinación y distribución de los mencionados recursos, determina a su vez la eficiencia y la economía del Proyecto.
Los planes del equipo auditor se desarrolla de la siguiente manera:
Eligiendo el responsable de la auditoria su propio equipo de trabajo. Este ha de ser heterogéneo en cuanto a especialidad, pero compacto.

Recabando de la empresa auditada los nombres de las personas de la misma que han de relacionarse con los auditores, para las peticiones de información, coordinación de entrevistas. Mediante un estudio inicial, del cual forma parte el análisis de un formulario exhaustivo, también inicial, que los auditores entregan al cliente para su cumplimentación.
Según los planes marcados, el equipo auditor, cumplidos los requisitos 1, 2 y 3, estará en disposición de comenzar la "tarea de campo", la operativa auditora del Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN _Finanzas

Ponderación de los Sectores Auditados
Este constituye la Fase 2 del Proyecto y engloba las siguientes actividades:
FASE 2. Ponderación de sectores del Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN _Finanzas

1. Asignación de pesos técnicos. Se entienden por tales las ponderaciones que el equipo auditor hace de los segmentos y secciones, en función de su importancia.
2. Asignación de pesos políticos. Son las mismas ponderaciones anteriores, pero evaluadas por el cliente.
3. Asignación de pesos finales a los Segmentos y Secciones. El peso final es el promedio del peso técnico y del peso político. La Subsecciones se calculan pero no se ponderan.

Se pondera la importancia relativa de la seguridad en los diversos sectores de la organización informática auditada.

Las asignaciones de pesos a Secciones y Segmentos del área de seguridad que se audita, se realizan del siguiente modo:

Pesos técnicos

Son los coeficientes que el equipo auditor asigna a los Segmentos y a las Secciones.

Pesos políticos

Son los coeficientes o pesos que el cliente concede a cada Segmento y a cada Sección del Ciclo de seguridad en BaaN _Finanzas en BaaN Finanzas.

Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN _Finanzas . Suma Pesos Segmentos = 100 (con independencia del número de segmentos consideradas)			
Segmentos	Pesos Técnicos	Pesos Políticos	Pesos Finales
Seg1. Normas y Estándares	12	8	10
Seg2. Sistema Operativo	10	10	10
Seg3. Software Básico	10	14	12
Seg4. Comunicaciones	12	12	12

Seg5. Bases de Datos	12	12	12
Seg6. Procesos	16	12	14
Seg7. Aplicaciones	16	16	16
Seg8. Seguridad Física	12	16	14
TOTAL	**100**	**100**	**100**

Pesos finales

Son el promedio de los pesos anteriores.

El total de los pesos de los 8 segmentos es 100. Este total de 100 puntos es el que se ha asignado a la totalidad del área de Seguridad, como podría haberse elegido otro cualquiera. El total de puntos se mantiene cualquiera que hubiera sido el número de segmentos. Si hubieran existido cinco segmentos, en lugar de 8, la suma de los cinco habría de seguir siendo de 100 puntos.

Suma Peso Secciones = 20 (con independencia del número de Secciones consideradas)			
Secciones	**Pesos Técnicos**	**Pesos Políticos**	**Pesos Finales**
Secc1. Seg. Física de Datos	6	6	6
Secc2. Control de Accesos	5	3	4
Secc3. Equipos	6	4	5
Secc4. Documentos	2	4	3
Secc5. Suministros	1	3	2
TOTAL	20	20	20

Puede observarse la diferente apreciación de pesos por parte del cliente y del equipo auditor. Mientras éstos estiman que las Normas y Estándares y los Procesos son muy importantes, el cliente no los considera tanto, a la vez que prima, tal vez excesivamente, el Software Básico.

Del mismo modo, se concede a todos los segmentos el mismo valor total que se desee, por ejemplo 20, con absoluta independencia del número de Secciones que tenga cada Segmento. En este caso, se han definido y pesado cinco Secciones del Segmento de Seguridad Física. Cabe aclarar, solo se desarrolló un solo Segmento a modo de ejemplo.

Operativa del Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN _Finanzas

Una vez asignados los pesos finales a todos los Segmentos y Secciones, se comienza la Fase 3, que implica las siguientes actividades:

FASE 3. Operativa Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN _Finanzas

Preparación y confirmación de entrevistas.

Entrevistas, pruebas, análisis de la información, cruzamiento y repaso de la misma.

Las entrevistas deben realizarse con exactitud. El responsable del equipo auditor designará a un encargado, dependiendo del área de la entrevista. Este, por supuesto, deberá conocer a fondo la misma.

La realización de entrevistas adecuadas constituye uno delos factores fundamentales del éxito de la auditoria. La adecuación comienza con la completa cooperación del entrevistado. Si esta no se produce, el responsable lo hará saber al cliente.

Deben realizarse varias entrevistas del mismo tema, al menos a dos o tres niveles jerárquicos distintos. El mismo auditor puede, y en ocasiones es conveniente, entrevistar a la misma persona sobre distintos temas. Las entrevistas deben realizarse de acuerdo con el plan establecido, aunque se pueden llegar a agregar algunas adicionales y sin planificación.

La entrevista concreta suele abarcar subsecciones de una misma Sección o una sección completa. Comenzada la entrevista, el auditor o auditores formulan las

preguntas al / los entrevistados, identificándose quien ha dicho qué, cuando son más de una las personas entrevistadas.

Se aplican listas de chequeo. Terminadas las entrevistas, el auditor califica las respuestas del auditado (no debe estar presente) y procede al levantamiento de la información correspondiente.

Simultáneamente a las entrevistas, el equipo auditor realiza pruebas planeadas y pruebas sorpresa para verificar y cruzar los datos solicitados y facilitados por el cliente. Estas pruebas se realizan ejecutando trabajos propios o repitiendo los de aquél, que indefectiblemente deberán ser similares si se han reproducido las condiciones de carga de los Sistemas auditados. Si las pruebas realizadas por el equipo auditor no fueran consistentes con la información facilitada por el auditado, se deberá recabar nueva información y reverificar los resultados de las pruebas auditoras.

La evaluación de las Checklists, las pruebas realizadas, la información facilitada por el cliente y el análisis de todos los datos disponibles, configuran todos los elementos necesarios para calcular y establecer los resultados de la auditoria, que se materializarán en el informe final.

A continuación, un ejemplo de auditoría de la Sección de Control de Accesos del Segmento de Seguridad Física:

La Sección de Control de Accesos a usuarios se divide en dos Subsecciones:

- Autorizaciones
- Registros

En las siguientes Checklists, las respuestas se calificarán de 1 a 5, siendo1 la más deficiente y 5 la máxima puntuación.

Control de Accesos: **Autorizaciones**		
Preguntas	Respuestas	Puntos
¿Existe un único responsable de implementar la política de autorizaciones de entrada en el Centro de Cálculo?	Si, el Jefe de Departamento de Información Científica, pero el Director puede acceder a la Sala con acompañantes sin previo aviso.	4
¿Existe alguna autorización permanente de estancia de personal ajeno a la empresa?	Una sola. El técnico permanente de la firma suministradora.	5
¿Quiénes saben cuales son las personas autorizadas?	El personal de vigilancia y el Jefe de Departamento de TI.	5
Además de la tarjeta magnética de identificación, ¿hay que pasar otra especial?	No, solamente la primera.	4
¿Se pregunta a las visitas si piensan visitar el Centro de Cálculo?	No, vale la primera autorización.	3
¿Se proveen las visitas al Centro de Cálculo con 24 horas al menos?	No, basta que vayan acompañados por el Jefe de Explotación o Director	3
TOTAL AUTORIZACIONES		**24/30 80%**

Control de Accesos: **Registros**		
Preguntas	Respuestas	Puntos
¿Existe una adecuada política de registros?	No, reconocemos que casi nunca, pero hasta ahora no ha habido necesidad.	1

¿Se ha registrado alguna vez a una persona?	Nunca.	1
¿Se abren todos los paquetes dirigidos a personas concretas y no a Informática?	Casi nunca.	1
¿Hay un cuarto para abrir los paquetes?	Si, pero no se usa siempre.	3
TOTAL REGISTROS		**6/20 30%**

Cálculos y Resultados Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN Finanzas.

FASE 4. Cálculos y resultados del Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN Finanzas

Cálculo y ponderación de Secciones y Segmentos. Las Sucesiones no se ponderan, solo se calculan.
Identificación de materias mejorables.
Priorización de mejoras.
En el punto anterior se han realizado las entrevistas y se han puntuado las respuestas de toda la auditoria de Seguridad.

El trabajo de levantamiento de información está concluido y contrastado con las pruebas. A partir de ese momento, el equipo auditor tiene en su poder todos los datos necesarios para elaborar el informe final. Solo faltaría calcular el porcentaje de bondad de cada área; éste se obtiene calculando la suma de las respuestas obtenidas, recordando que deben afectarse a sus pesos correspondientes. Una vez

realizado los cálculos, se ordenaran y clasificaran los resultados obtenidos por materias mejorables, estableciendo prioridades de actuación para lograrlas.

Cálculo del ejemplo de las Subsecciones de la Sección de Control de Accesos:
Autorizaciones 80%
Registros 30%

Promedio de Control de Accesos 62,5%.
Cabe recordar, que dentro del Segmento de Seguridad Física, la Sección de Control de Accesos tiene un peso final de 4.

Prosiguiendo con el ejemplo, se procedió a la evaluación delas otras cuatro Secciones, obteniéndose los siguientes resultados:

Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN Finanzas: **Segmento 8, Seguridad Física.**		
Secciones	Peso	Puntos
Sección 1. Datos	6	57,5%
Sección 2. Control de Accesos	4	62,5%
Sección 3. Equipos (Centro de Cálculo)	5	70%
Sección 4. Documentos	3	52,5%
Sección 5. Suministros	2	47,2%

Conocidas los promedios y los pesos de las cinco Secciones, se procede a calcular y ponderar el Segmento 8 de Seguridad Física:

Seg. 8 = PromedioSección1 * peso + PromedioSecc2 * peso +PromSecc3 * peso + PromSecc4 * peso + PromSecc5 * peso / (peso1 + peso2 + peso3+ peso4 + peso5) ó
Seg. 8 = (57,5 * 6) + (62,5 * 4) + (70 * 5) + (52,5 * 3) +(47,2 * 2) / 20

Seg. 8 = 59,85%

A continuación, la evaluación final de los demás Segmentos del ciclo de seguridad en BaaN _Finanzas en BaaN Finanzas:

Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN_Finanzas. Evaluación y pesos de Segmentos		
Segmentos	Pesos	Evaluación
Seg1. Normas y Estándares	10	61%
Seg2. Sistema Operativo	10	90%
Seg3. Software Básico	12	72%
Seg4. Comunicaciones	12	55%
Seg5. Bases de Datos	12	77,5%
Seg6. Procesos	14	51,2%
Seg7. Aplicaciones	16	50,5%
Seg8. Seguridad Física	14	59,8%
Promedio Total Área de Seguridad	**100**	**63,3%**

Sistemática seguida para el cálculo y evaluación del Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN_Finanzas:

Valoración de las respuestas a las preguntas específicas realizadas en las entrevistas y a los cuestionarios formulados por escrito.

Cálculo matemático de todas las subsecciones de cada sección, como media aritmética (promedio final) de las preguntas específicas. Recuérdese que las subsecciones no se ponderan.

Cálculo matemático de la Sección, como media aritmética (promedio final) de sus Subsecciones. La Sección calculada tiene su peso correspondiente.
Cálculo matemático del Segmento. Cada una de las Secciones que lo componen se afecta por su peso correspondiente. El resultado es el valor del Segmento, el cual, a su vez, tiene asignado su peso.

Cálculo matemático de la auditoría. Se multiplica cada valor de los Segmentos por sus pesos correspondientes, la suma total obtenida se divide por el valor fijo asignado a priori a la suma de los pesos de los segmentos.

Finalmente, se procede a mostrar las áreas auditadas con gráficos de barras, exponiéndose primero los Segmentos, luego las Secciones y por último las Subsecciones. En todos los casos sé hará una referencia con respecto a tres zonas: roja, amarilla y verde.

La **zona roja** corresponde a una situación de debilidad que requiere acciones a corto plazo. Serán las más prioritarias, tanto en la exposición del Informe como en la toma de medidas para la corrección.

La **zona amarilla** corresponde a una situación discreta que requiere acciones a medio plazo, figurando a continuación de las contenidas en la zona roja.

La **zona verde** requiere solamente alguna acción de mantenimiento a largo plazo.

Nula	Pobre	Insuficiente	Sufic.	Adecuado	buena	Excel.

Confección del Informe del Ciclo de Seguridad de Derechos a los Usuarios al Módulo BaaN_Finanzas

Fase5. *Confección del informe del* **Ciclo de Seguridad de Derechos a los Usuarios al Módulo**

BaaN_Finanzas
Preparación de borrador de informe y Recomendaciones.
Discusión del borrador con el cliente.
Entrega del Informe y Carta de Introducción.

Ha de resaltarse la importancia de la discusión de los borradores parciales con el cliente. La referencia al cliente debe entenderse como a los responsables directos de los segmentos. Es de destacar que si hubiese acuerdo, es posible que el auditado redacte un contrainforme del punto cuestionado. Esta acta se incorporará al Informe Final.

Las Recomendaciones del Informe son de tres tipos:
Recomendaciones correspondientes a la zona roja. Serán muy detalladas e irán en primer lugar, con la máxima prioridad. La redacción de las recomendaciones se hará dé modo que sea simple verificar el cumplimiento de la misma por parte del cliente.

Recomendaciones correspondientes a la zona amarilla. Son las que deben observarse a medio plazo, e igualmente irán prior izadas.

Recomendaciones correspondientes a la zona verde. Suelen referirse a medidas de mantenimiento. Pueden ser omitidas. Puede detallarse alguna de este tipo cuando una acción sencilla y económica pueda originar beneficios importantes.

Entorno tecnológico: Se refiere a contar con la más sofisticada tecnología suministrada por los principales proveedores a escala mundial. En otras palabras se

extrae la mejor tecnología y se aplica a la realidad empresarial. Entorno de innovación:

Se refiere al análisis del entorno y cómo se utiliza éste para proporcionar oportunidades de transferencia de tecnología. El control interno se define como un proceso, efectuado por todo el personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable. Entorno de control: establece el tono de la institución al influenciar la conciencia de control de su personal Evaluación de riesgos identifica el proceso gerencial para el establecimiento de los objetivos institucionales y los riesgos asociados al logro de dichos objetivos, y determina si los riesgos son manejados adecuadamente.

Empresas:
Dos o más personas que trabajan juntas de manera estructurada para alcanzar una meta o una serie de metas específicas.

Efectividad:
Método para comparar hechos de acuerdo a los propósitos generales. Observa el comportamiento de la toma de la decisión.

Eficacia:
Ponderación del grado de cumplimiento de los objetivos específicos formulados en alguna oportunidad previa. Tiene que ver con la calidad del producto obtenido.

Eficiencia:
Valorización de resultados en función del gasto empleado para obtener el beneficio buscado. Esta referido al costo, su dimensión y la capacidad para garantizar la sostenibilidad del emprendimiento.
Información y comunicación: Establece cómo la organización identifica, captura e intercambia información de una forma y en un período de tiempo que le permita a las personas llevar a cabo sus responsabilidades.

Sistemas:
Es un todo organizado con lógica, en que el funcionamiento global es mayor que la suma de sus partes.

Sistemas de información estratégicas: Son el uso de la tecnología de la información para soportar o dar forma a la estrategia competitiva de la organización, a su plan para incrementar o mantener la ventaja competitiva o bien para reducir la ventaja de sus rivales.

Supervisión:
Identifica el proceso utilizado por la organización para determinar o medir la calidad del desempeño de la estructura de control interno a través del tiempo.
Delimitación en el tiempo y en el espacio con explicación de razones que lo justifican. P Esto lo hacemos considerando la importancia de la implantación de sistemas de gestión BaaN en las empresas y la incidencia de los mismos en la eficiencia y eficacia de las actividades que realizan.

2.5 Ejercicio para la comprobación de los informes financieros de consolidación del Módulo BaaN Finanzas.

Se realizaron acciones con el objetivo de revisar el comportamiento de las integraciones de los informes financieros de consolidación del Módulo Baan Finanzas. Ellas consistieron en lo siguiente:

- Chequeo del listado de dimensiones de los centros de costo definidos en BaaN, para comprobar que coincide con el listado aprobado.
- Chequeo de los saldos totales del Balance de Comprobación de Saldos en el período auditado, comprobando que coinciden.
- Chequeo de los saldos de las cuentas en el período auditado, verificando que corresponden a su naturaleza contable.
- Revisión de que todas las cuentas contables tengan definido el campo Tipo de Cuenta que las relaciona con el Balance General o con el Estado de Resultados.
- Chequeo de las referencias de la cuentas a sus cuentas contables padres.

- Revisión de que todos los tipos de variables definidas tengan correctos parámetros de integración y elementos de integración.
- Revisión de los tipos de asientos definidos y sus propiedades.
- Revisión de que en el listado de artículos, todos los elementos tengan definidos los grupos contables de proveedores, almacén, familias de artículos, artículo, descripción y componentes del costo.
- Revisar que no existan asientos no finalizados en el período.
- Revisión de que todos los activos tengan establecido su grupo de activos, código de amortización contable, método de amortización, datos de configuración inicial, datos maestros, tipo de transacción y estado.
- Revisar el reporte de errores de UNIx
- Listar el resumen de la cuenta 70320 Cuenta de redondeo- Compensación.

Los resultados obtenidos de esta revisión muestran que la información primaria está libre de representación errónea de importancia relativa en lo que concierne a los objetivos de la auditoria informática del sistema de gestión, de conformidad con normas y principios de contabilidad generalmente aceptados.

CONCLUSIONES

Durante nuestra revisión se pudo observar que los controles generales del Sistema operaron de manera efectiva durante el periodo correspondiente a la auditoria y por lo tanto soportan de manera confiable el procesamiento de la información financiera de la Empresa auditada Pedro Sotto Alba. Existiendo confianza razonable en la información que se obtiene del ambiente de procesamiento.

Fueron identificadas un número de mejoras a aplicar para robustecer el control en el ambiente de procesamiento en general.

El resultado de nuestra evaluación nos indica que efectivamente se puede utilizar la información generada bajo el ambiente de procesamiento del Sistema Informático la empresa Pedro Sotto Alba para soportar la auditoria informática al 31 de diciembre del 2005.

Como resultado, también se evidenció la necesidad de efectuar personalizaciones, las cuales se realizaron, aportando un valor adicional al trabajo realizado.

RECOMENDACIONES

Teniendo en cuenta las conclusiones anteriores y debido a la importancia que posee esta investigación para realizar una Auditoria Informática a cualquier centro de Información país recomendamos:

1. Implementar las mejoras identificadas.
2. Indicar a la empresa y a los usuarios de la información contable que esta puede ser utilizada en función de las necesidades de información que estos tengan.
3. Continuar estudiando el ambiente de control y el sistema de para que sea más flexibles, eficaces y efectivos para mejorar procesamiento de información, identificando otras necesidades de personalizaciones la calidad del control de la contabilidad de la empresa.
4. Programar reportes mas flexible para los usuarios del sistemas BaaN, por los diferentes Módulos.

BIBLIOGRAFÍA

1. Carmona Gonzáles, M., La Auditoria Interna de Gestión: Aspectos Técnicos. El caso particular cubano., España, 2001.
2. Carmona Gonzáles, M., Control Interno., Cuba
3. Ramos Baissalier, Ramon., Revista del Banco Central de Cuba., Gestión de Riesgos. **Tecnología** que se impone., Publicación Centro de Información bancaria y Economica (CIDE)., Publicación trimestral enero-marzo, 2000.
4. Oficina Nacional de Auditoria., Regulaciones y normas de Auditoria., Republica de Cuba., Resolución ONA-2/97 del 25/11/97.
5. Blanco Encinaza, Lázaro J., La auditoria informática al comienzo del tercer milenio., GIGA. La Revista Cubana de computación: Colombus Conectividad., Nº6, 2000.
6. Revista PC WORLD. Los Secretos del nuevo Office. Edición julio 2001 Panamá, año 8 número 101.
7. Revista PC WORLD. Proteja su PC, como evitar ataque de virus. Edición julio 2002. Panamá, año 10, número 112.
8. Carmona Gonzáles, M., Control Interno., Cuba
9. Ramos Baissalier, Ramon., Revista del Banco Central de Cuba., Gestión de Riesgos. **Tecnología** que se impone., Publicación Centro de Información bancaria y Economica (CIDE)., Publicación trimestral enero-marzo, 2000.
10. Oficina Nacional de Auditoria., Regulaciones y normas de Auditoria., Republica de Cuba., Resolución ONA-2/97 del 25/11/97.
11. Blanco Encinaza, Lázaro J., La auditoria informática al comienzo del tercer milenio., GIGA. La Revista Cubana de computación: Colombus Conectividad., Nº6, 2000.
12. Revista PC WORLD. Los Secretos del nuevo Office. Edición julio 2001 Panamá, año 8 número 101.
13. Revista PC WORLD. Proteja su PC, como evitar ataque de virus. Edición julio 2002. Panamá, año 10, número 112.

- **Direcciones de Internet Revisadas**

http://cache.fdo-may.ubiobio.cl/decom/doc/VIRUS2.htm

http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

http://dmi.uib.es/~bbuades/auditoria/auditoria.PPT

http://www.delitosinformaticos.com/propiedadindustrial/auditoria.shtml

http://www.monografías.com/trabajos11/breverres/breverres.shtml

http://www.monografías.com/trabajos/seguinfo/seguinfo/shtml

http://www.geocities.com/Athens/Olympus/7428/virus1.html

http://www.criptored.upm.es/guiateoria/gt_m142a.htm

http://www.notariado.org/noticias/escriturapublica/16%20escriturapublica/la@2.htm

http://pp.terra.com.mx/ hugalde/virussoy.html

http://www.belt.es/articulos/articulo.asp?id=65

http://www.ctv.es/USERS/mpq/estrado/estrado004.html

GLOSARIO

Glosario de Términos Económicos

Alcance de la auditoría. El marco o límite de la auditoría y las materias, temas, segmentos o actividades que son objeto de la misma.

Amortización. Cancelación sistemática del costo de un activo intangible por el vencimiento del tiempo establecido como término de su usufructo

Auditores externos. Profesionales facultados que no son empleados de la organización cuyas afirmaciones o declaraciones auditan.

Auditores internos. Profesionales empleados por una organización para examinar continuamente y evaluar el sistema de control interno y presentar los resultados de su investigación y recomendaciones a la alta dirección de la entidad.

Auditoría. Técnica de control, dirigida a valorar, el control interno y la observancia de los Principios Profesionales de Contabilidad Generalmente Aceptados. Comprende un examen independiente de los registros de contabilidad y otra evidencia relacionada con una entidad para apoyar la opinión experta imparcial sobre la confiabilidad de los estados financieros.

Base de datos. Un centro de almacenamiento de información dentro de un sistema contable computarizado. La idea de una base de datos consiste en la información que va a tener una variedad de usos y que, se registra en el sistema computarizado una sola vez, en ese momento la información se almacena en una base de datos. Luego, a medida que se necesite, el computador puede recuperarla de la base de datos y colocarla en el formato deseado.

Control interno. Todas las medidas utilizadas por una empresa para protegerse contra errores, desperdicios o fraudes y para asegurar la confiabilidad de los datos contables. Está diseñado para ayudar a la operación eficiente de una empresa y para asegurar el cumplimiento de las políticas de la empresa.

Entidad (empresarial). Una unidad económica que realiza transacciones comerciales que se deben registrar, resumir y reportar. Se considera la entidad separada de su propietario o propietarios.

Hallazgos. Son el resultado de un proceso de recopilación y síntesis de información: la suma y la organización lógica de información relacionada con la entidad, actividad, situación o asunto que se haya revisado o evaluado para llegar a conclusiones al respecto o para cumplir alguno de los objetivos

de la auditoría. Sirven de fundamento a las conclusiones del auditor y a las recomendaciones que formula para que se adopten las medidas correctivas.

Informe de auditoría. Expresión escrita por el auditor respecto a los resultados de las verificaciones realizadas durante la ejecución de la auditoría, manifestando sus criterios y comentarios respecto a los estados financieros y otros hechos económicos.

Informe de los auditores. El informe emitido después de auditar un tema o los estados financieros de una empresa

Objetivo de la auditoría. Propósito o fin que persigue la auditoría, o la pregunta que se desea contestar por medio de la auditoría

Técnicas de auditoría. Métodos que el auditor emplea para realizar las verificaciones planteadas en los programas de auditoría, que tienen como objetivo la obtención de evidencia.

Transacciones entre compañías. Transacciones entre dos compañías afiliadas. Los efectos en las transacciones entre compañías, tales como préstamos entre compañías se eliminan como un paso al preparar los estados financieros consolidados.

ANEXOS

Anexo 1. Bitácoras de Servidores

UNÍx

* 14/02/05 P1-C1 Fallo el CPU del servidor AixTest : Tenia Sucio y
corrosión.

* Cuando un usuario nuevo no entra y al probarlo en el servidor da error en la línea 84 del script hay que revisar pues su nombre es parte de otro nombre: por ejemplo: eperez es parte de reperez y la solución es cambiar uno de los dos nombres.

Novell

140305 Al tratar de restaurar los datos de geología daba insuficiente espacio en disco: Restaure primero sin los derechos y luego restaure los derechos. Esto es en las propiedades del RestaureNetware: no restaurar derechos.

Citrix

==========

Content Advisor is a feature in Internet Explorer that allows supervisors to restrict the web sites that the users can browse. The supervisor can set a password in order to prevent from other users from changing the Content Advisor properties.

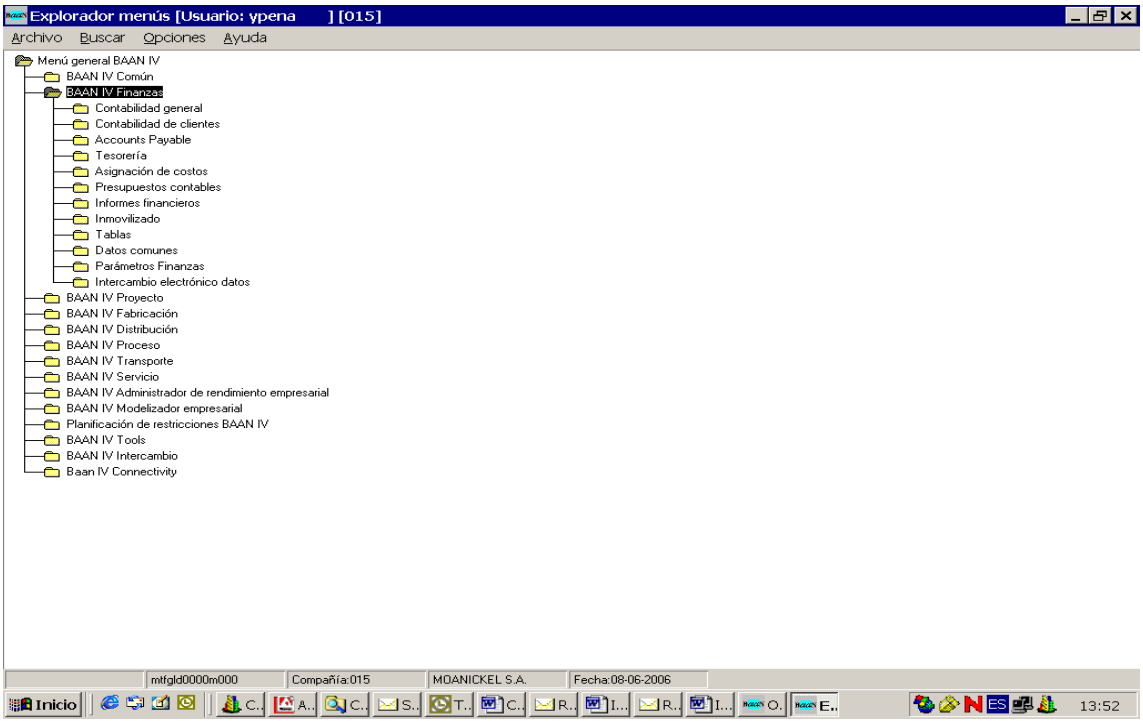
If the supervisor forgets the password, he cannot change the Content Advisor properties in the regular way. The simplest way to solve this problem is to delete the password in the Registry.

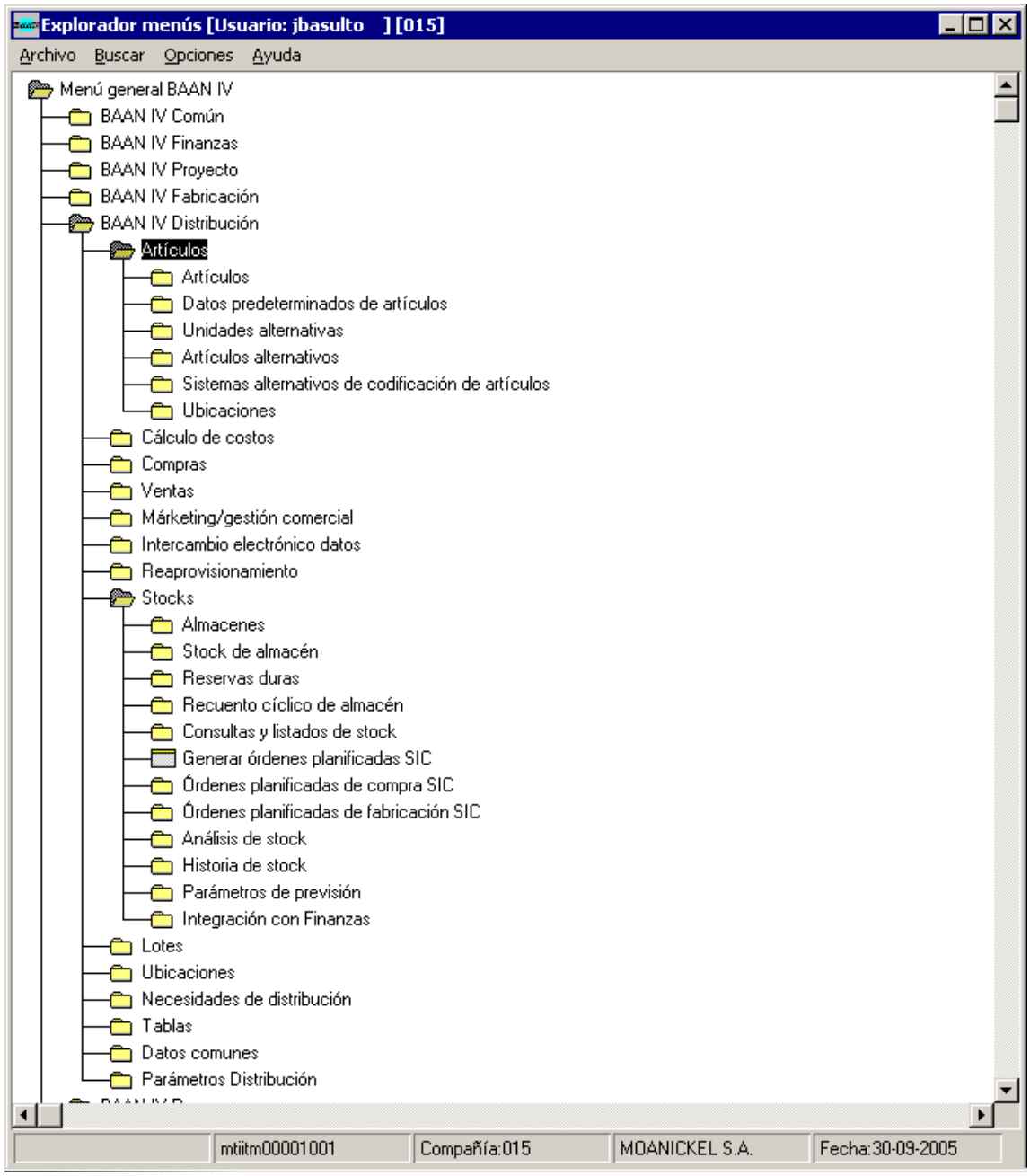
The password is stored in HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Ratings. The "Key" value represents the encrypted password.

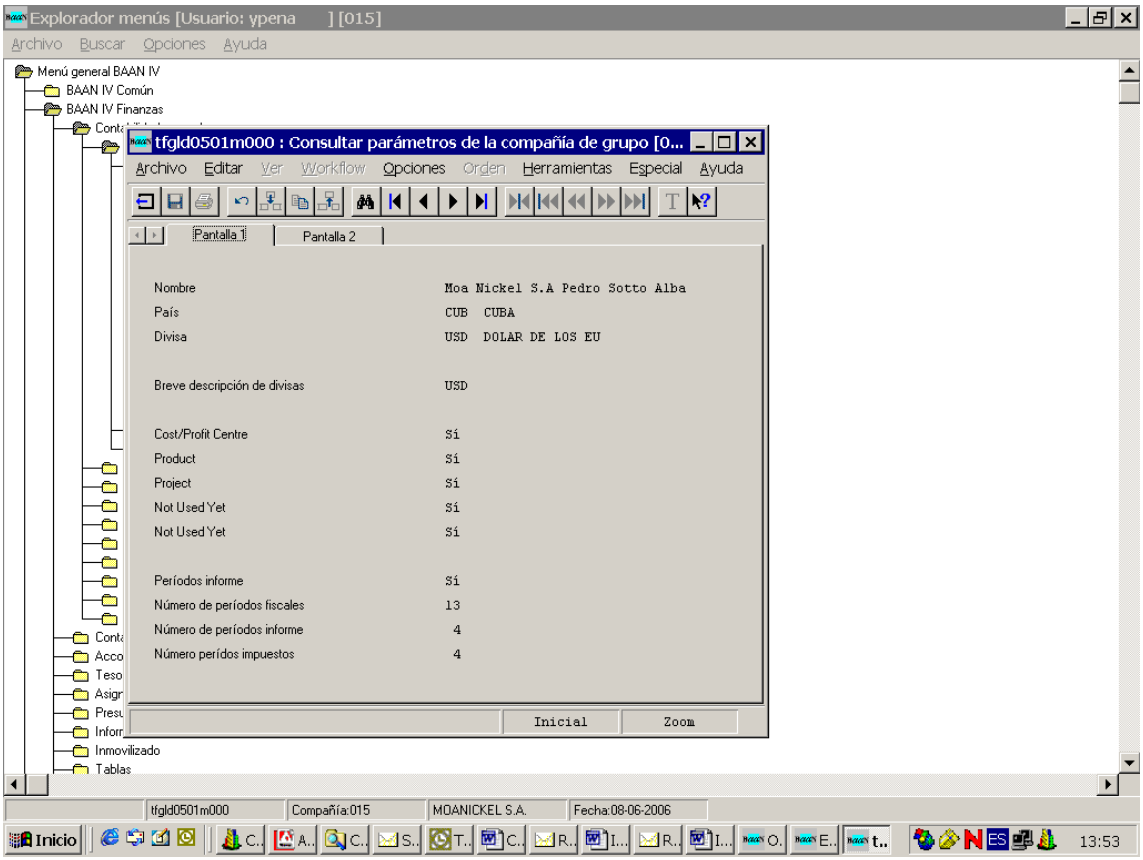
Advanced users can easily delete the password from the registry and thus they don't need this utility.

User who doesn't wan15/01/05 No funciona el storage en metaframe debido a un error en ora.tns: se puso una copia desde administ : pelota

ANEXO 2. Menus del Sistema SSA-BaaN de Global.


Explorador menús [Usuario: ypena] [015]
Archivo Buscar Opciones Ayuda
Menú general BAAN IV
BAAN IV Común
BAAN IV Finanzas
Contabilidad general
Contabilidad de clientes
Accounts Payable
Tesorería
Asignación de costos
Presupuestos contables
Informes financieros
Inmovilizado
Tablas
Datos comunes
Parámetros Finanzas
Intercambio electrónico datos
BAAN IV Proyecto
BAAN IV Fabricación
BAAN IV Distribución
BAAN IV Proceso
BAAN IV Transporte
BAAN IV Servicio
BAAN IV Administrador de rendimiento empresarial
BAAN IV Modelizador empresarial
Planificación de restricciones BAAN IV
BAAN IV Tools
BAAN IV Intercambio
Baan IV Connectivity
mtfgld0000m000
Compañía:015
MOANICKEL S.A.
Fecha:08-06-2006
Inicio
13:52


Explorador menús [Usuario: jbasulto] [015]
Archivo Buscar Opciones Ayuda
Menú general BAAN IV
BAAN IV Común
BAAN IV Finanzas
BAAN IV Proyecto
BAAN IV Fabricación
BAAN IV Distribución
Artículos
Artículos
Datos predeterminados de artículos
Unidades alternativas
Artículos alternativos
Sistemas alternativos de codificación de artículos
Ubicaciones
Cálculo de costos
Compras
Ventas
Márketing/gestión comercial
Intercambio electrónico datos
Reaprovisionamiento
Stocks
Almacenes
Stock de almacén
Reservas duras
Recuento cíclico de almacén
Consultas y listados de stock
Generar órdenes planificadas SIC
Órdenes planificadas de compra SIC
Órdenes planificadas de fabricación SIC
Análisis de stock
Historia de stock
Parámetros de previsión
Integración con Finanzas
Lotes
Ubicaciones
Necesidades de distribución
Tablas
Datos comunes
Parámetros Distribución
mtiitm00001001
Compañía:015
MOANICKEL S.A.
Fecha:30-09-2005



Anexo 3: Resumen de cuentas

Anexo 4: Resumen de cuentas por Países

Anexos 5: Derechos de usuarios en BaaN

Anexos 6: Saldo de comprobación (Cuentas contables).

Anexo 7: Maestro de Periodo.

Anexo 8: Listados de errores de Finalización.

Anexo 9: Tipos de asientos

Anexo 10: Balance de comprobación por cuentas.

Anexo 11 :Maestros y Dimensiones