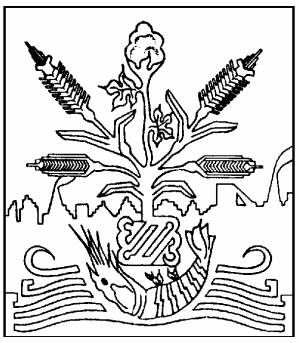


INSTITUTO TECNOLÓGICO DE SONORA

APLICACIÓN DE UNA AUDITORÍA OFIMÁTICA EN LA EMPRESA "LA CASITA" DEDICADA A LA CONSTRUCCIÓN DE FRACCIONAMIENTOS Y VIVIENDAS DE INTERÉS SOCIAL

TESIS QUE PARA OBTENER EL TÍTULO DE

LICENCIADO EN SISTEMAS DE INFORMACIÓN ADMINISTRATIVA

PRESENTAN

ELIANNA VILLA VALDEZ

NIDIA MONDRAGÓN OROZCO

CD. OBREGÓN, SONORA NOVIEMBRE 2000

DEDICATORIAS

A MIS PADRES:

Roque Villa López y María Elia Valdez Luque, quienes me han ayudado a salir adelante con su apoyo incondicional y por estar siempre a mi lado cuando más los he necesitado, siendo para mi un gran estímulo para seguir superándome constantemente y llegar a alcanzar todas las metas que me he planteado. Les dedico este trabajo con mucho amor, ya que es uno de los primeros frutos que han surgido en mi vida para ustedes y el comienzo de muchos más. Los quiero mucho!!!

A MIS HERMANOS:

Roque y Rogelio, por haber estado siempre bien unidos como una muy bonita familia que somos, disfrutando tantos fines de semana viendo películas y comiendo las deliciosas "Botanas". Espero ser un buen ejemplo a seguir, así como lo son ustedes para mi y los admiro mucho por ser como son.

A LA FAMILIA VILLA:

A todos y cada uno de ellos, ya que hemos estado compartiendo muchos momentos muy agradables y felices en el transcurso de toda la vida, principalmente en la tradicional Rosca de Reyes, y aunque casi no nos visitemos recuerden que siempre están en mi mente y en mi corazón. Especialmente a mis tías: Laura y Yoly que estuvieron cuidándome en todo el transcurso de mi vida, dándome sus consejos que han sido muy importantes para mi.

A LA FAMILIA VALDEZ ("LOS GORGOJOS"):

A todos los Gorgojos por estar conviviendo en las buenas y en las malas muchos momentos que hemos tenido, principalmente a todos mis primos (que son muchos), que hemos estado

conviviendo cada vez que se puede en Casa Blanca y hemos disfrutado cada etapa de nuestras vidas.

A MIS ABUELAS:

Mamá Teofila, Mamá Constanza y por supuesto a mi Bisabuela del alma: Mamá Chayo, les dedico este trabajo que significa la culminación de mis estudios y el comienzo de mi nueva vida esperando que se sientan muy orgullosas de mi y recuerden que las quiero muchísimo

A MI NIÑO:

Por haber sido uno de mis mejores amigos dentro de mi carrera, ya que estuvimos juntos desde el primer día hasta la culminación de ella, empezando como simplemente amigos hasta llegar a lo que somos hoy: una gran pareja!

A DOÑA EVA:

Porque en el tiempo que la conozco ha sido para mi más que una amiga, ha sido como parte de mi familia (a parte de todo el tiempo que me la he llevado en su casa y todas las comidas que me ha dado), llegándola a querer más de lo que se imagina.

A MIS AMIGOS:

Tanto dentro y fuera de mi carrera, porque han estado acompañándome en varios momentos de mi vida: en discos, reuniones, fiestas, “Carnes Asadas”, fiestas, etc., y sobre todo en las famosas “Juntas de Equipo” que estuvieron en cada clase de nuestra carrera, así como las múltiples tareas, entre otras cosas que surgían a medida que nos desenvolvíamos profesionalmente.

A LAS DEL CAFÉ:

Por hacer ese día (no específico cual, por estarse cambiando constantemente) que ayuda a que no se apague nuestra amistad y seguir siempre juntas. Especialmente a ti Lizeth por haber sido mi mejor amiga, que me ayudó con sus consejos a superar tristezas y que estuvo en mis alegrías, las idas al “Barce”, a comer o desayunar fueron muy placenteras para mi. A ti Mayra por tus múltiples ocurrencias y sobre todo en las veces que salíamos y salimos juntas. MaryPaz o más bien “María de la Paz” (jeje), que aunque casi no vas al café también estás dentro de él, por preocuparte por mi, estar conmigo, bueno les dedico esto ¡a todas en general!

Elianna Villa Valdez

AGRADECIMIENTOS

A DIOS:

Por darme la fuerza suficiente para seguir adelante y mostrarme el camino que tengo que seguir para superarme constantemente. Le doy gracias por ayudarme a levantar cuando me he caído. Por estar conmigo siempre y en cada lugar.

A MIS PADRES:

Porque son un ejemplo a seguir para mi y siempre me han ayudado a romper los obstáculos que han estado en mi vida y haber logrado superarlos, ya sea con sus palabras de aliento y por qué no? Por haberme tendido la mano cuando la he necesitado. Pero sobre todo por haberme dado la vida, que sin ella no soy nada.

A MIS HERMANOS:

Porque en ellos veo que tienen un gran futuro, son muy inteligentes y son capaces de muchas cosas, ayudándome a superarme cada vez más, para que ellos también vean en mi lo que yo veo en ellos.

A MI NIÑO:

Te agradezco por estar siempre a mi lado cuando lo he necesitado, por contar con tu apoyo, amor y dedicación hacia mi, por todo: TE AMO!

A LA FAMILIA FIGUEROA ECHEGARAY:

Especialmente a Doña Eva, por todas las veces que nos tuvo que soportar en las juntas de equipo que teníamos en su casa y las veces que he comido en ella y a su familia por estar

brindándome parte de sus risas y felicidad cuando estoy con ustedes. ¡Espero que no se hayan enfadado!

MARIOLY:

Por haberme ayudado en el transcurso de mi carrera con la experiencia que ella adquirió en la suya. Te agradezco por haber sido mi “hermana ” en el tiempo que vivimos juntas y por ser grandes amigas desde la infancia hasta ahora.

A NIDIA MONDRAGÓN:

Por haber hecho esto juntas, logrando así la culminación de nuestra carrera y el inicio de una nueva vida, además de ser gran compañera y amiga, que esto no sea el fin de nuestra amistad, sino el inicio de ella.

A MI ASESORA:

Lic. Anabel Morimoto Barbuzón, por habernos ayudado en la realización de este trabajo que fue de gran ayuda para nosotras, así como al haber sido más que una maestra ha sido una gran amiga

AL COODINADOR DE NUESTRA CARRERA:

Al maestro Federico Gámez Villegas por habernos ayudado en la culminación de nuestra carrera al habernos orientado en los procesos de titulación y en las revisiones correspondientes de nuestro trabajo.

Elianna Villa Valdez

DEDICATORIAS

A MIS PAPÁS:

Quiero dedicarle este trabajo a mis papás, porque esto es parte del fruto de lo que ellos han cosechado a través de mí, quiero ofrecerles mi trabajo y estudios de toda la vida y ojalá que se sientan orgullosos por haber logrado en mí a una profesional, espero ahora empezar otra etapa de mi vida.

A MIS HERMANAS Y CUÑADOS:

Les dedico este trabajo para que conozcan un poco de lo que su hermana y cuñada ha estado estudiando a través de toda la carrera.

A MI SOBRINO:

También quiero dedicarle unas palabras a mi sobrino: “Te dejo el reto ahora a Ti”.

A MIS AMIGOS:

Quiero decirles que a través de esta parte de mi vida, que hoy culmino, hay muchas experiencias con ustedes y muchos momentos felices, espero que existan por mucho tiempo más. Espero que para los que no han terminado, esto les sirve un poco de ejemplo. Al Victor le agradezco y le dedico este trabajo porque siempre me ayudó durante toda la carrera, quién sabe que hubiera sido de mí en todas las materias de programación. Gracias también por ser mi amigo.

Nidia Mondragón Orozco

AGRADECIMIENTOS

A DIOS:

Le doy las gracias primeramente a dios por haberme dado la vida y haberme permitido llegar hasta este momento tan importante en mi vida, además de tener la capacidad de realizar una carrera de estudios durante toda una vida.

A MIS PAPÁS:

Porque siempre han querido que esté bien preparada y me han dado la oportunidad de estudiar y poder concluir sin problema alguno.

A MIS HERMANAS:

Les agradezco que me hayan dejado un reto por cumplir ya que ustedes ya lo realizaron. Este reto hoy lo cumplo “titularme”.

A MIS AMIGAS:

Porque siempre han estado conmigo en todos los momentos y por ser parte de esto que hoy termino, Carolina especialmente quiero darte las gracias por todos los momentos en que estuviste conmigo.

A ELIANNA:

Por haberme dado la oportunidad de formar parte en la realización de este trabajo y por la amistad que siempre me ha ofrecido en las buenas y en las malas, espero que nunca termine.

A MI ASESORA:

Lic. Annabel Morimoto Barbuzón, por el tiempo que nos dedicó y la ayuda que siempre nos ofreció para que este trabajo resultara bueno.

AL COORDINADOR DE LA CARRERA:

Por habernos infundado el valor de querer que siempre concluyéramos con nuestra carrera y de la mejor forma. También por la atención brindado en los momentos de asesoría y trámites.

Nidia Mondragón Orozco

RESUMEN

La Auditoría de la Ofimática es un término poco conocido por las empresas y es por ello que no se lleva a cabo en las organizaciones como ésta debería. Si las empresas la realizaran regularmente en su organización, podrían estar enteradas de cómo está funcionando, saber si su inventario de cómputo y sus aplicaciones están siendo utilizados de una manera eficaz y eficiente, y sobre todo saber si están llevando un buen procedimiento para la adquisición de nuevos productos, así como saber si la seguridad que se utiliza es la más adecuada. En el presente trabajo se realizó una Auditoría de la Ofimática para conocer si el aprovechamiento de los recursos Ofimáticos en la empresa "La Casita" son o no los adecuados, donde se entrevistó al Jefe de Desarrollo de Sistemas y al Administrador de la Red, quienes conocen los Sistemas de Información y los procedimientos de adquisición de equipo de cómputo y aplicaciones de toda la organización. A ellos también se les solicitó contestar un cuestionario de 99 preguntas que contenía aspectos como: economía, eficacia, eficiencia y seguridad, que fueron los puntos clave en está investigación. Además de la entrevista y cuestionario se revisó la documentación, equipo de cómputo y sus aplicaciones, así como los formatos que utilizaban para el inventario, compra, solicitud de servicio, que fueron de gran utilidad para la elaboración del presente, dictaminándose el resultado correspondiente, siendo éste, una ***opinión con salvedades*** debido al incumplimiento de la normativa legal al no contar con las licencias correspondientes a aplicaciones que se utilizan dentro de la organización. Sin embargo, esto no llega a afectar significativamente a la empresa debido a que no altera el buen funcionamiento de los procedimientos, pero sí económicamente y legalmente en caso de que fueran detectadas todas las aplicaciones utilizadas sin licencia. Por lo tanto, se concluye que el aprovechamiento de los recursos ofimáticos en esta empresa son los adecuados.

ÍNDICE

CAPÍTULO I

INTRODUCCIÓN

En las organizaciones se está teniendo en claro la importancia de estarse actualizando y de estar siempre a la vanguardia en el manejo de la información, es por ello que la mayoría de las empresas están implantando en sus instalaciones, aplicaciones y equipos de cómputo que los ayuden a agilizar sus procesos y mejorar la rapidez con la que fluye la información, todo esto sin tomar en cuenta lo que implica.

Al contar con aplicaciones y equipo de cómputo dentro de la organización, el personal de la empresa sólo se centra en que éstos solamente cumplan con el propósito por el que fueron implantados sin ver los beneficios que se pueden obtener al realizar posteriormente una auditoría ofimática.

En este capítulo se analizará la importancia de realizar una auditoría ofimática dentro de las organizaciones, para que puedan aprovechar al máximo todas sus aplicaciones y equipo.

1.1 Antecedentes.

El motivo de la investigación que se pretende realizar surgió a raíz del conocimiento adquirido en la materia de Auditoría de Sistemas de Información en el último semestre de la carrera de Licenciado en Sistemas de Información Administrativa, al realizar un trabajo parcial sobre el tema de la Auditoría Ofimática.

Posteriormente, se analizaron diferentes empresas en las que se pudiera realizar la auditoría ofimática, y una vez analizados los requisitos para realizar ésta, se seleccionó a la empresa "La Casita", dedicada a la construcción de fraccionamientos y viviendas, siendo la idónea para auditarla. Al haber visitado la empresa en cuestión, se le planteó todo el proceso a seguir para realizar la auditoria ofimática, aceptando que le sería de provecho realizarla en sus instalaciones para mejorar el uso de sus recursos ofimáticos, brindando toda la información necesaria para llevarla a cabo.

El concepto de ofimática, según Piattini y Del Peso, (1998) nace al percibirse la necesidad de automatizar los procesos y tareas administrativas por medio de los sistemas de información. El funcionamiento de las oficinas apoyadas por el área de sistemas de información ha logrado un espectacular crecimiento en la demanda de sistemas ofimáticos y que hoy en día continúan acrecentándose. Ejemplos de sistemas ofimáticos son: aplicaciones específicas para la gestión de tareas, procesadores de texto, hojas de cálculo, control de expedientes, sistemas de almacenamiento de información, bases de datos, correo electrónico, agendas personales.

El impacto que estos sistemas de información han producido en la actualidad, provoca una constante evolución en el desarrollo de los sistemas ofimáticos, esto ha ocasionado que las empresas se preocupen por el funcionamiento del equipo de cómputo y las diversas aplicaciones que utilizan; es por ello que realizar una Auditoría Ofimática ayudará a generar, procesar, recuperar, comunicar y presentar datos relacionados con el funcionamiento de la oficina.

Esta investigación tiene el fin de proporcionar las herramientas necesarias para que una organización pueda aprovechar al máximo todas sus aplicaciones ofimáticas y tenga una mejor distribución de información en diferentes departamentos.

1.2 Justificación.

La necesidad de llevar un control de todo lo referente al entorno microinformático, justifica el presente trabajo, donde se analizará la distribución de las aplicaciones y del equipo en los diferentes departamentos de la organización, ayudando a la empresa a reducir sus costos, y evitar el desaprovechamiento de lo que se tiene o de que lo que se va a adquirir.

Esta investigación se realiza para dar a conocer si la empresa carece de eficiencia y rapidez en los procesos, falta de ordenadores personales y estaciones de trabajo, si cuenta con actualizaciones de aplicaciones ofimáticas, y la insatisfacción de los usuarios al manejar las aplicaciones; aprovechamiento adecuado de los contratos de garantía; si cuentan con suficientes métodos de seguridad.

Las implicaciones que pueden resultar al realizar una auditoría en este tipo de entornos son: adquisiciones poco planeadas; desarrollos ineficaces e ineficientes; procesos críticos para el correcto funcionamiento de la organización; advertir a los usuarios la falta de conciencia acerca de la seguridad de la información; la utilización de copias ilegales en las aplicaciones; procedimientos de copias seguridad deficientes; falta de capacitación al personal; ausencia de documentación; malos inventarios y mal aprovechamiento de garantías.

Los beneficios obtenidos serán directamente para la organización puesto que a los directivos de la empresa les interesa conocer cómo tener una mejora en el manejo del equipo de trabajo, saber si el proceso que siguen para la adquisición del equipo y aplicaciones son los adecuados, conocer si cuentan con buenos métodos de seguridad, además de observar la inversión de equipo informático en los activos de la empresa, logrando con esto un aumento en la productividad y una reducción de costos.

El tipo de investigación es descriptiva, ya que la finalidad de ésta es dar a conocer un diagnóstico de cómo se encuentra actualmente la empresa en cuanto al aprovechamiento de los recursos ofimáticos.

1.3 Planteamiento del problema.

Algunos aspectos que la gerencia de un negocio considera importantes son: la optimización de recursos; ahorro de tiempo; eficiencia y rapidez en los procesos. Éstos se pueden lograr con una buena auditoría de la ofimática. Al no tener controles, las empresas difícilmente detectan ciertas fallas, lo que ha ocasionado problemas en eficiencia, eficacia y seguridad, trayendo con ello repercusiones a nivel organizacional.

Una vez analizados los resultados arrojados por la investigación se proporcionarán nuevas alternativas para la solución de los problemas que se tengan en la empresa, de esta manera los altos niveles de la organización obtendrán la información necesaria para llevar a cabo una buena toma de decisiones.

Con esto se pretende evitar que las organizaciones tengan un mal manejo de sus sistemas ofimáticos, obteniendo con eso que sus procesos y tareas se vean afectados, ocasionando un retraso en todas sus operaciones diarias, debido a que el entorno ofimático maneja todos los procedimientos más utilizados en las empresas.

Al dar un informe con resultados y recomendaciones se podrá tomar decisiones de gran trascendencia para la empresa, como lo es un mejor control en la adquisición de nuevos equipos y aplicaciones, una relación más efectiva de todo el inventario, información actualizada, equipo realmente efectivo, rapidez en los procesos con el fin de que la empresa evite pérdidas de tiempo, malos funcionamientos, carencia de equipos y aplicaciones para su funcionamiento. Pero una auditoría de la ofimática: ¿Puede solucionar que una empresa tenga bien inventariado su equipo de cómputo? ¿Mantenga siempre sus actualizaciones de software? ¿Tenga la suficiente seguridad en los equipos y en el acceso a los sistemas de información? ¿Realice sus compras de nuevo equipo porque se ha analizado que se necesitan? ¿El equipo satisface realmente las necesidades que el puesto requiere?

1.4. Hipótesis.

La hipótesis ayuda a precisar los problemas y establecer los datos que deben tomarse en cuenta para someterse a prueba y así aprobarla o rechazarla. La formulación de una hipótesis depende primordialmente de su objetivo principal, la relativa al presente trabajo de investigación se expresa a continuación:

Hi: Al aplicar la Auditoría de la Ofimática se conocerá si el aprovechamiento de los recursos ofimáticos en esta empresa son los adecuados.

Ho: Al aplicar la Auditoría de la Ofimática se conocerá si el aprovechamiento de los recursos ofimáticos en esta empresa no son los adecuados.

Al realizar esta investigación, se hará válida alguna de las hipótesis antes planteadas.

1.5. Objetivo.

El propósito general de esta investigación es proporcionar las herramientas necesarias para que una organización pueda aprovechar al máximo todas sus aplicaciones ofimáticas y tenga una mejor distribución de información en los diferentes departamentos.

Se manejarán los criterios de seguridad, eficiencia en el manejo de la información, eficacia en los procesos para llevar a cabo la auditoría ofimática con el fin de obtener resultados que sirvan como referencia para realizar futuros cambios en la empresa.

Los objetivos específicos que se derivan de esta investigación:

- Determinar si el inventario ofimático refleja con exactitud los equipos y aplicaciones existentes en la organización.
- Determinar y evaluar el procedimiento de adquisiciones de equipos y aplicaciones.
- Determinar y evaluar la política de mantenimiento definida en la organización.
- Evaluar la calidad de las aplicaciones del entorno ofimático desarrollada por personal de la propia organización.

- ♣ Evaluar la corrección del procedimiento existente para la realización de los cambios de versiones y aplicaciones.
- ♣ Determinar si los usuarios cuentan con suficiente formación y la documentación de apoyo necesaria para desarrollar sus tareas de un modo eficiente.
- ♣ Determinar si el sistema existente se ajusta a las necesidades reales de la organización.
- ♣ Determinar si existen garantías suficientes para proteger los accesos no autorizados a la información reservada de la empresa y la integridad de la información.
- ♣ Determinar si el procedimiento de generación de copias de respaldo es fiable y garantiza la recuperación de la información en caso de necesidad.
- ♣ Determinar si está garantizado el funcionamiento ininterrumpido de aquellas aplicaciones cuya caída podría suponer pérdidas de integridad de la información y aplicaciones.
- ♣ Determinar el grado de exposición ante la posibilidad de intrusión de virus.
- ♣ Determinar si en el entorno ofimático se producen situaciones que pueden provocar infracciones.

Con estos objetivos, se evaluará si el aprovechamiento de los recursos ofimáticos en esta empresa son o no son los adecuados.

1.6. Importancia del estudio

En la actualidad, las organizaciones quieren mantenerse actualizadas implementando los sistemas de información, sin embargo los sistemas no son debidamente analizados al aplicarse por lo que existen deficiencias en cuanto a la compra y manejo de los mismos, obteniendo así deficiencias para la organización.

El valor que representa la información actualmente es de gran importancia, por lo tanto las organizaciones tienen que estar seguras de lo que obtienen debido a que las inversiones en estas tecnologías son costosas y la mala obtención de ellas puede ocasionar pérdidas tanto de capital como de información.

Al realizar una auditoría ofimática se puede tener un mejor control de todas las aplicaciones que se utilizan dentro de una organización, de esta forma las personas que laboran dentro de la misma adquieren un mayor conocimiento del equipo y de las aplicaciones con que cuenta para desempeñar de la mejor manera su trabajo, utilizando eficientemente todos sus recursos y capacidades.

La aportación de los conocimientos hacia las personas que se dedican al área de sistemas, sería tener una base para observar los problemas que se tuvieron al realizar esta investigación, así como la metodología que se utilizó para realizarla. Esta investigación no soluciona los problemas de la comunidad pero ayuda a que la empresa, como en este caso dedicada a la construcción de fraccionamientos y viviendas de interés social, mejore sus servicios de información hacia el cliente ayudando a que éste quede satisfecho con la información brindada.

El criterio a utilizar es de relevancia contemporánea, porque al aplicarse una auditoría ofimática, se contribuye a la realización de un estudio que la organización no contempla, ya que solo se limita a la implantación de los sistemas y no se encarga de estudiar más a fondo todos los beneficios y provechos que se pueden obtener.

1.7 Limitaciones del estudio.

Las limitaciones encontradas para este estudio son:

- Imposibilidad de accesar a inventarios reales.
- No tener acceso al equipo de cómputo.
- Sólo puede ser aplicada a oficinas que cuenten con equipo de cómputo y aplicaciones.
- Carencia de la documentación necesaria por parte de la organización, como son: contratos de mantenimiento, licencias de aplicaciones, registros de compra.
- Por motivo de la confidencialidad de la información, se manejará un nombre ficticio en lo que respecta al nombre original de la empresa.
- Sólo aplica a este tipo de empresas.
- Falta de información acerca de este tema.

Contar con alguna de estas limitaciones hará que los resultados que se obtengan no sean lo más cercano a la realidad, pero no impide que se realice el estudio y se tengan resultados.

CAPÍTULO II

REVISIÓN BIBLIOGRÁFICA

Es importante conocer la documentación teórica necesaria para la comprensión del presente estudio, es por ello que en este capítulo se verán los conceptos y procedimientos que serán de gran utilidad para tener una visión más clara de los puntos que se tratan en toda la investigación, siendo los principales:

- ♣ Auditoría Informática
- ♣ Herramientas y Técnicas para la Auditoría Informática
- ♣ Ofimática
- ♣ Controles de Auditoría Informática
- ♣ El informe de Auditoría.

Este capítulo ofrece a cualquier lector que no tenga conocimiento del tema, una explicación sencilla y fácil de entender de los puntos que se mencionaron, así como los que se desglosan de ellos.

2.1 Auditoría.

Piattini y Del Peso, (1998) definen conceptualmente a la Auditoría como la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.

Se puede analizar descomponer este concepto en los elementos fundamentales que a continuación se especifican:

1) contenido: una opinión
2) condición: profesional
3) justificación: sustentada en determinados procedimientos
4) objeto: una determinada información obtenida en un cierto soporte
5) finalidad: determinar si presenta adecuadamente la realidad o ésta responde a las expectativas que le son atribuidas, es decir, su fiabilidad.

En todo caso es una función que se acomete a posteriori, en relación con actividades ya realizadas, sobre las que hay que emitir una opinión.

2.2 Clases de Auditoría.

Según Piattini y Del Peso, (1998) el objeto sometido a estudio, sea cual sea su soporte, por una parte, y la finalidad con que se realiza el estudio, define el tipo de Auditoría de que se trata. A título ilustrativo se podrían enumerar entre otras:

Tabla 2.1 "Clases de Auditoría"

CLASE	CONTENIDO	OBJETO	FINALIDAD
Financiera	Opinión	Cuentas anuales	Presentan realidad
Informática	Opinión	Sistemas de aplicación, recursos informáticos, planes de contingencia, etc.	Operatividad eficiente y según normas establecidas.
Gestión	Opinión	Dirección	Eficacia, eficiencia, economicidad
Cumplimiento	Opinión	Normas establecidas	Las operaciones se adecuan a estas normas

Es interesante aclarar que hay herramientas de software de ayuda a la Auditoría de cuentas que aunque se les llamen herramientas de Auditoría, sólo lo son para los auditores de cuentas, y esto no es Auditoría informática sino ayuda a la Auditoría de cuentas.

Es decir, que no es lo mismo ser un informático de los auditores que ser auditor informático. La Auditoría financiera es un dictamen sobre los estados de cuentas. Y la Auditoría informática es una Auditoría en sí misma, y si el auditor informático no certifica la integridad de los datos informáticos que usan los auditores financieros, éstos no deben usar los sistemas de información para sus dictámenes. Tal es la importancia de la existencia de los auditores informáticos, que son los gerentes de la veracidad de los informes de los auditores financieros que trabajan con los datos de los sistemas de información.

2.3 Definición de Informática.

La Informática es una disciplina que abarca desde el estudio teórico de modelos, algoritmos y procesamiento de información hasta la producción de software eficiente y confiable para satisfacer los requerimientos de una organización.

Tiene como foco central a los procesos de manejo y manipulación de información, con el interés particular de hacerlos más eficientes y dotarlos de cierta inteligencia. Anónimo, (1998).

2.4 Auditoría Informática o Auditoría de Sistemas de Información.

Según Piattini y Del Peso, (1998) la Auditoría informática es el proceso de recolectar, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. De este modo la Auditoría informática sustenta y confirma la consecución de los objetivos tradicionales de la Auditoría:

- ♣ Objetivos de protección de activos e integridad de los datos.
- ♣ Objetivos de gestión que abarcan, no solamente los de protección de activos sino también los de eficacia y eficiencia.

La Auditoría informática es un conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un sistema informático, con el fin de proteger sus actividades y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general en cada empresa, y para conseguir la eficacia exigida en el marco de la organización correspondiente.

2.5 Herramientas y Técnicas para la Auditoría Informática.

Existen diversas herramientas y técnicas para obtener datos y poder llevar a cabo una auditoría. A continuación se describen según Canaves, (1999).

2.5.1 Cuestionarios. Las auditorías informáticas 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 la realización de cuestionarios 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.

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 auditoría.

Cabe aclarar, que esta primera fase puede omitirse cuando los auditores hayan adquirido por otro medios la información que aquellos cuestionarios hubieran proporcionado, por ejemplo a través de entrevistas.

2.5.2 <u>Entrevistas.</u> El auditor comienza las relaciones personales con el auditado. Lo hace de tres formas:

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

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recibe más información que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a 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. Tras ella debe existir una preparación elaborada y sistematizada, y que es diferente para cada caso particular.

2.5.3 Checklist. 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, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para la realización sistemática de sus Cuestionarios, de sus Checklists.

Hay opiniones de personas que han utilizado los Checklist y descalifican el uso de éstos, ya que consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático. Pero esto no es usar Checklists, es una evidente falta de profesionalismo, ya que pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. Por lo tanto éste posee preguntas muy estudiadas que han de formularse flexiblemente.

El conjunto de estas preguntas recibe el nombre de Checklist. Salvo excepciones, los Checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

Según la claridad de las preguntas y el 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, aún siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el modo y el orden de su formulación. Las empresas externas de Auditoría 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 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 utilizadas para cada sector, deben ser repetidas. En efecto, bajo apariencia distinta, el auditor formulará preguntas equivalentes a las mismas o a distintas personas, 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.

2.6 La Ofimática.

La definición realizada por Piatinni y Del Peso, (1998) entendiendo ofimática como el sistema informatizado que genera, procesa, almacena, recupera, comunica y presenta datos relacionados con el funcionamiento de la oficina.

El concepto de ofimática nace a comienzos de la década pasada y las primeras aplicaciones se desarrollan sobre los ordenadores centrales de las organizaciones. Aunque las oficinas siempre han sido consideradas como pioneras en la utilización de herramientas informáticas para el desarrollo de actividades; desde comienzos de los noventa se ha producido un espectacular crecimiento en la demanda de sistemas ofimáticos que todavía continúa acrecentándose. Ejemplos de ellos son: las aplicaciones específicas para la gestión de tareas, como hojas de cálculo o procesadores de textos; herramientas para la gestión de documentos, como control de expedientes o sistemas de almacenamiento óptico de información; agendas y

bases de datos personales; sistemas de trabajo en grupo como el correo electrónico o el control de flujos de trabajos, etc.

2.7 Controles de Auditoría Ofimática.

Según Piattini y Del Peso, (1998) los controles que se presentan agrupados siguiendo criterios relacionados con aspectos de economía, eficacia y eficiencia; seguridad y condicionantes legales, son suficientemente generales para servir de base en la elaboración del guión de trabajo de la labor del equipo auditor. A continuación se describen los aspectos a evaluar de la auditoría ofimática:

2.7.1 Economía, eficacia y eficiencia. En este punto se comprueba por medio de los auditores que la empresa maneje correctamente los siguientes aspectos:

Determinar si el inventario ofimático refleja con exactitud los equipos y aplicaciones existentes en la organización.

A causa del bajo costo de muchos componentes, resulta difícil mantener un registro fiable de todas las compras que realiza la organización. Con frecuencia algunos de los departamentos sortean los procedimientos y autorizaciones de compra establecidos dentro de la organización, por ejemplo, utilizando facturas de adquisición de material no inventariable.

Un inventario poco fiable puede repercutir en el balance de la organización, con la posibilidad de que no se detecten sustracciones de equipamiento informático o de licencias de programas contratadas. Se ha seleccionado este control en primer lugar, ya que la fiabilidad del inventario resultará indispensable para auditar otros controles presentados posteriormente.

El equipo auditor comprobará que se han definido mecanismos para garantizar que todos los equipos adquiridos en la organización son debidamente inventariados. Después, constatará a la conciliación realizada en la última Auditoría financiera entre el inventario oficial y las adquisiciones efectuadas. Más tarde, revisando todas las dependencias, almacenes y archivos,

elaborará una relación exhaustiva de los equipos informáticos y de las aplicaciones y ficheros que residen de los mismos. En esta relación deben quedar reflejadas también la versión correspondiente a cada una de las aplicaciones instaladas. Finalmente, identificará las diferencias reales entre la relación elaborada por el equipo auditor y el inventario oficial para proceder a la subsanación de los errores detectados.

Determinar y evaluar el procedimiento de adquisiciones de equipos y aplicaciones.

Una política de adquisiciones descentralizada en la que cada departamento se encargue de realizar sus compras, ofrece ventajas en cuanto a flexibilidad y capacidad de reacción de los mismos, pero podría acarrear significativas pérdidas económicas para el conjunto de la organización.

El equipo auditor comprobará que en el procedimiento de adquisición se valoran aspectos relativos a la necesidad real de los equipos solicitados y a la integración de dichos equipos con el sistema existente. En el caso de compra de paquetes o de contratación de desarrollos externos, determinará si las prestaciones ofrecidas por el producto solicitado se ajustan a las actividades que se pretendan desarrollar con el; si las plataformas en las que se van a ser instaladas las aplicaciones tienen suficiente capacidad para soportarlas de un modo eficiente; si los nuevos productos pueden configurarse en caso de necesidad, para obtener suficientes pistas de Auditoría que permitan efectuar un seguimiento de las anomalías producidas entre su ejecución; la experiencia y solvencia del proveedor.

Partiendo del inventario debidamente actualizado, analizará los procedimientos para la adquisición de los productos seguidos en los diversos departamentos de la organización y determinará la existencia de equipos y aplicaciones similares. En caso de que los diversos departamentos de la compañía realicen pedidos sobre equipos y complementos de manera independiente, estudiará si se está desaprovechando la posibilidad de negociar descuentos mediante la aplicación de una política centralizada de compras. Del mismo modo, considerará otros mecanismos que pudieran reducir los costos de la organización como podría ser la negociación centralizada de la compra de licencia de aplicaciones.

Determinar y evaluar la política de mantenimiento definida en la organización.

Los procedimientos descentralizados han propiciado que, en ocasiones, los equipos adquiridos no sean incluidos ni en el inventario ni en los contratos de mantenimiento, incluso

podría llegar a suceder que el personal de la organización encargado del mantenimiento no dispusiera de los conocimientos necesarios para llevarlo a cabo.

El equipo auditor examinará la utilización de las garantías de los productos adquiridos comprobando que no se realizan pagos innecesarios por asistencias de equipos y aplicaciones que se encuentren en garantía. Para ello, deberá verificar que los usuarios finales conocen el estado de las garantías de cada uno de los productos que utilizan y los mecanismos para hacerlas efectivas.

Por lo que respecta a productos cuya garantía haya caducado, determinará cuáles disponen de contratos de mantenimiento vigentes con empresas externas y cuáles son aquellos en los que la responsabilidad del mantenimiento recae en la propia organización. En las contrataciones de mantenimiento con empresas externas verificará si se han incluido en el contrato aspectos como el tiempo máximo de respuesta, recambios y mano de obra, mantenimiento preventivo, etc. También comprobará que el personal, tanto interno como externo, asignado en tareas de mantenimiento tiene suficientes conocimientos de las plataformas que debe mantener, y que recibe la información adecuada sobre los nuevos productos instalados en la organización.

En relación con la gestión de incidencias producidas, el equipo auditor comprobará la existencia de un registro de las mismas, los procedimientos establecidos para asignar recursos para solucionarlas, los guiones preparados para solventar las incidencias más frecuentes y el seguimiento de las mismas hasta su resolución. También valorará si el tiempo empleado para atender las solicitudes y resolver las incidencias producidas puede llegar a afectar al funcionamiento de la organización.

Evaluar la calidad de las aplicaciones del entorno ofimático desarrollada por el personal de la propia organización.

La utilización de herramientas ofimáticas por los usuarios finales ha propiciado el desarrollo de aplicaciones, en muchos casos sin las debidas garantías de fiabilidad, cuyo mal funcionamiento puede repercutir significativamente a la actividad de la organización cuando se trate de aplicaciones que gestionen procesos críticos. Por otra parte, también es común que los desarrollos en estos entornos no hayan seguido los controles de calidad y seguridad suficientes, posibilitando que algún programador haya introducido “puertas traseras”, bombas lógicas o cualquier otro mecanismo que pudiera perturbar el buen funcionamiento de la aplicación desarrollada.

El equipo auditor determinará la existencia de un departamento responsable de controlar el desarrollo de aplicaciones de toda la organización, y que se han definido procedimientos generales de petición, autorización, asignación de prioridades, programación y entrega de aplicaciones, o bien si los departamentos han desarrollado aplicaciones de uso interno, bajo sus propios criterios, sin control de un departamento responsable. En caso de desarrollos realizados por el personal de los propios departamentos, el equipo auditor tendrá que determinar si la metodología empleada y los test de pruebas se ajustan a lo dispuesto en la organización.

Al igual que en el caso de las aplicaciones adquiridas o desarrolladas fuera de la organización, comprobará que las aplicaciones desarrolladas internamente pueden configurarse para obtener las suficientes pistas de Auditoría que permitan efectuar un seguimiento de las anomalías producidas durante su ejecución. Asimismo, verificará que los desarrollos se realizan sobre un entorno de desarrollo, evitando operar directamente sobre los datos reales de explotación.

También es tarea del equipo auditor examinar el reporte de incidencias de las aplicaciones, así como las reclamaciones manifestadas por los clientes y usuarios como indicios para detectar aquellas aplicaciones que podrían estar funcionando de un modo anómalo.

Evaluar la corrección del procedimiento existente para la realización de los cambios de versiones y aplicaciones.

Los cambios de aplicaciones o de versiones pueden producir situaciones de falta de integración y de incompatibilidad entre los nuevos productos instalados y los existentes con anterioridad. Prácticamente la totalidad de las nuevas versiones son capaces de manejar los formatos utilizados por versiones anteriores, pero no siempre ocurre en sentido contrario.

El equipo auditor determinará la existencia de procedimientos formalmente establecidos para la autorización, aprobación, adquisición de nuevas aplicaciones y cambios de versiones. Así mismo comprobará que las aplicaciones instaladas y los cambios de versiones han seguido todos los trámites exigidos en el procedimiento establecido.

También se ocupará de determinar si se han analizado los problemas de integración y las incompatibilidades que pueden plantear los nuevos productos previamente a su implantación; si se ha establecido algún plan para la formación de los usuarios finales que vayan a utilizar estos nuevos productos; y si los encargados de mantenerlos han adquirido los conocimientos

suficientes para que los cambios que van a producirse no impacten negativamente en el funcionamiento de la organización.

Determinar si los usuarios cuentan con suficiente formación y la documentación de apoyo necesaria para desarrollar sus tareas de un modo eficaz y eficiente.

Un conocimiento deficiente de las funcionalidades de las aplicaciones por parte de los usuarios finales o de los encargados del mantenimiento, puede ocasionar pérdida de eficacia y eficiencia en la utilización de las mismas. No se debe olvidar que carecer de los conocimientos necesarios puede ser debido, tanto a que los usuarios no han sido formados, como a que no han aprovechado debidamente los cursos de formación recibidos.

El equipo auditor determinará la existencia de un plan de formación para garantizar que todo el personal conoce los productos que tiene que utilizar, incluyendo las nuevas aplicaciones y las versiones instaladas. También comprobará que tras la realización de los cursos, se aplica algún mecanismo para determinar el aprovechamiento conseguido, y si se entrega a los usuarios la documentación básica de la operativa del producto, o si pueden acceder a ella fácilmente en caso de necesidad.

Igualmente, comprobará que los empleados utilizan las posibilidades que ofrece el producto y no simulan procedimientos utilizados en versiones previas o en aplicaciones utilizadas con anterioridad. Asimismo, evaluará los mecanismos y circuitos establecidos para solucionar las dudas y problemas planteados, determinando si la responsabilidad de solucionarlos corresponde a un equipo de soporte común a toda la organización, o bien, recae sobre el propio departamento.

Determinar si el sistema existente se ajusta a las necesidades reales de la organización.

La existencia de equipos obsoletos o infrautilizados puede ocasionar situaciones que, por mala distribución de los equipos a las necesidades de la organización, repercutan en el correcto funcionamiento de la misma.

El equipo auditor valorará el uso que se realiza de los equipos existentes, elaborando una relación de aquellos ordenadores que no se encuentren operativos. Asimismo, revisará las actividades que se ejecutan en cada equipo, determinando aquellos puestos de trabajo que, por las tareas que desempeñan, necesitan ser automatizados o precisan actualizar los equipos existentes; así como aquellos puestos que, debido a su escasa actividad, se encuentran sobredimensionados.

A la vista de los resultados obtenidos, elaborará una relación con recomendaciones sobre la descatalogación de productos obsoletos, redistribuciones y adquisiciones de nuevos equipos y aplicaciones.

2.7.2 <u>Seguridad.</u> En este punto se comprueba por medio de los auditores que la empresa maneje correctamente los siguientes aspectos:

Determinar si existen garantías suficientes para proteger los accesos no autorizados a la información reservada de la empresa y la integridad de la misma.

Las aplicaciones ofimáticas gestionan información reservada como agendas de contactos, informes sobre temas confidenciales, estadísticas obtenidas con información extraída de la base de datos corporativa, etc. Los accesos no autorizados o las inconsistencias en este tipo de información pueden comprometer el buen funcionamiento de la organización.

Las funcionalidades en materia de seguridad de las aplicaciones ofimáticas y los sistemas operativos de los ordenadores personales se han incrementado significativamente en los últimos años, ofreciendo un nivel de seguridad aceptable. No obstante, garantizar el cumplimiento de algunas de las medidas de seguridad expuesta a continuación exigirá recurrir a la adquisición de paquetes adicionales y, la adopción de medidas organizativas.

El equipo auditor examinará la documentación en materia de seguridad existente en la organización y comprobará que han sido definidos, al menos, procedimientos de clasificación de la información, control de acceso, identificación y autenticación, gestión de soportes, gestión de incidencias y controles de Auditoría. Con posterioridad pasará a comprobar si las medidas de seguridad definidas se encuentran realmente operativas.

En primer lugar, determinará si el procedimiento de clasificación de la información establecido ha sido elaborado atendiendo la sensibilidad e importancia de la misma, y comprobará que toda la información se ha clasificado en función de los criterios establecidos.

Tras verificar que las funciones, obligaciones y responsabilidades, en materia de la seguridad, de cada puesto de trabajo están claramente definidas y documentadas, comprobará que se han adoptado las medidas necesarias para que todo el personal conozca tanto aquellas que

afecten al desempeño de su actividad como las responsabilidades en que pudiera incurrir en caso de incumplirlas.

Examinando la relación actualizada de usuarios del sistema y de derechos de acceso establecidos, comprobará que cada usuario tiene autorización para acceder únicamente a aquellos datos y recursos informáticos que precisa para el desarrollo de sus funciones.

El equipo auditor deberá comprobar si se han establecido procedimientos de identificación y autenticación para el acceso al sistema. Cuando el segundo procedimiento se base en contraseñas, determinará si el procedimiento de creación, almacenamiento, distribución y modificación de las mismas garantiza su confidencialidad. También, determinará si los usuarios desconectan sus puestos de trabajo al finalizar la jornada, y si existe algún mecanismo que produzca la desconexión automática de un usuario tras un período de inactividad determinado, o bien, que precise introducir una contraseña para reanudar el trabajo.

En ningún caso olvidará verificar el cumplimiento de los procedimientos establecidos para solicitar nuevos accesos o modificaciones sobre los derechos definidos para un usuario, y que, exclusivamente, el personal autorizado se ocupará de conceder, alterar o anular los derechos de acceso sobre los datos y recursos informáticos.

El equipo auditor analizará el procedimiento de notificación y gestión de incidencias definido en la autorización, determinando cuáles son las incidencias registradas, el momento en que se producen, la persona que realiza la notificación, a quién le son comunicadas, el responsable asignado para revisarla y corregirla, los efectos producidos y las actuaciones que han provocado.

Finalmente, comprobará que todos los soportes informáticos permiten identificar la información que contienen, si son inventariados y si se almacenan en un lugar con acceso restringido únicamente al personal autorizado. Igualmente, verificará que la salida de soportes informáticos fuera de la organización es debidamente autorizada.

Determinar si el procedimiento de generación de las copias de respaldo es fiable y garantiza la recuperación de la información en caso de necesidad.

La información generada por el sistema debe estar disponible en todo momento. La no disponibilidad de datos, especialmente de aquellos procedimientos críticos para la organización, además de las consabidas pérdidas económicas, podría llevar, en el extremo, a la paralización del departamento.

El equipo auditor examinará el procedimiento de copias de seguridad seguido en la organización, verificando la suficiencia de la periodicidad, la correcta asignación de responsabilidades y el adecuado almacenamiento de los soportes.

En primer lugar, comprobará que la responsabilidad de realizar las copias de la seguridad está asignada y que cada responsable las realiza con la información que se encuentra bajo su responsabilidad, de tal forma que todos los datos son salvaguardados. A continuación, verificará la existencia de un inventario de los soportes que las contienen, así como de la información salvaguardada.

Posteriormente, determinará si la seguridad implementada para garantizar la confidencialidad e integridad de las copias de salvaguarda ofrece garantías equivalentes a las definidas para la información que contienen, tanto en los soportes que se mantienen en los locales de la empresa como en aquellos que se trasladan en una ubicación externa.

Finalmente, controlará la eficacia del procedimiento definido para la recuperación de las copias de seguridad, determinando si los soportes contienen información que está previsto que contengan, y si es posible la recuperación de la misma, de forma que el resultado final sea un fiel reflejo de la situación anterior.

Determinar si está garantizado el funcionamiento ininterrumpido de aquellas aplicaciones cuya caída podría suponer pérdidas de integridad de la información y aplicaciones.

En las organizaciones se desarrollan procesos en los que una caída de tensión podría ocasionar pérdidas de integridad de la información y aplicaciones manejadas, en ocasiones irrecuperables.

El equipo auditor determinará la existencia de sistemas de alimentación ininterrumpida, y si éstos cubren el funcionamiento de aquellos equipos en los que se ejecutan procesos cuya interrupción podría ocasionar graves repercusiones.

Asimismo, debe ocuparse de simular una caída de tensión, verificar si los equipos de alimentación ininterrumpida entran en funcionamiento y comprobar si el tiempo de actividad proporcionado por el sistema de alimentación ininterrumpida es suficiente para la finalización de los proceso críticos y la desconexión del sistema.

Determinar el grado de exposición ante la posibilidad de intrusión de virus.

Los costos derivados de la intrusión de virus informáticos se han multiplicado en los últimos años: pérdida de la información y empleo de recursos y tiempo para re-establecer el sistema, llegando en algunos casos a la paralización temporal del departamento.

El equipo auditor analizará la protección establecida en cada uno de los puntos del sistema por los que podrían introducirse virus: disqueteras, módems, accesos a redes, etc.; y revisará la normativa para la instalación y actualización periódica de productos antivirus, prestando especial atención a aquellos caso en que la información manejada puede ser crítica para el funcionamiento de la organización.

Asimismo, analizará la configuración de los equipos y la instalación de programas que permitan detectar la existencia de virus, evitar su intrusión en el sistema y eliminar aquellos que sean introducidos.

En caso de que detectara algún virus en alguno de los equipos, el equipo auditor informará inmediatamente al responsable autorizado sugiriendo las medidas que estime pertinentes para evitar la propagación del mismo.

Con esto se verificará que las empresas cuenten con la suficiente seguridad para mantener la integridad de la información.

2.7.3 Tipos de Seguridad. Según Seen, (1992) la seguridad es responsabilidad de todos aquellos que están en contacto con el sistema, y es tan buena como el comportamiento o política más laxa en la organización. La seguridad tiene tres aspectos interrelacionados: física, lógica y de comportamiento. Los tres deben trabajar juntos si se pretende que la calidad de la seguridad permanezca alta.

2.7.3.1 Seguridad Física. La seguridad física se refiere a la seguridad de las instalaciones de computación, su equipo y software por medios físicos. Esto puede incluir el control de acceso al cuarto de la computadora por medio de gafetes legibles por máquina o sistemas de registro/despedida humanos, el uso de cámaras de televisión de circuito cerrado para monitorear

las áreas de computadora y el respaldo de datos frecuente así como el almacenamiento de los respaldos en un área a prueba de fuego y agua.

Además, el equipo de cómputo pequeño debe estar asegurado para que un usuario típico no pueda moverlo, y se debe garantizar la corriente sin interrupciones. Las alarmas que notifican a las personas adecuadas, la presencia de fuego, inundaciones o intrusión humana no autorizada deben ser funcionales todo el tiempo.

Las decisiones acerca de la seguridad física deben tomarse cuando el analista está planeando las instalaciones de cómputo y la compra de equipo. Obviamente, la seguridad física puede ser mucho más fuerte si se piensa en ella antes de la instalación actual, y si los cuartos de la computadora están equipados especialmente para su seguridad cuando son construidos, en vez de ser acondicionados posteriormente.

2.7.3.2 Seguridad Lógica. Se refiere a los controles lógicos dentro del mismo software. Los controles lógicos familiares para la mayoría de los usuarios son contraseñas y códigos de autorización de algún tipo. Cuando son usados permiten que el usuario con la contraseña correcta entre al sistema o a una parte particular de la base de datos. Sin embargo, las contraseñas son tratadas desdeñosamente en muchas organizaciones. Se ha visto que los empleados gritan una contraseña a través de oficinas con mucha gente, escriben las contraseñas en papeles pegados en sus terminales (post-it) y comparten contraseñas personales con empleados autorizados que han olvidado la suya, haciendo insegura la información que se encuentra en su computadora y otras personas pueden hacer mal uso de ella.

Los controles lógicos y físicos son importantes, pero no son suficientes para proporcionar una seguridad adecuada. También se necesitan cambios de comportamiento.

2.7.3.3 Seguridad de comportamiento. Las expectativas de comportamiento de una organización están codificadas en sus manuales de política y hasta en signos puestos en tableros

de noticias. Pero el comportamiento que tienen internamente los miembros de la organización también es crítico para el éxito de los esfuerzos de la seguridad.

La seguridad puede comenzar por investigar a los empleados que eventualmente tendrán acceso a las computadoras, datos e información, para asegurarse de que sus intereses sean consistentes con los de la organización y que comprenden completamente la importancia de llevar a cabo procedimientos de seguridad. Las políticas que se refieren a seguridad deben ser escritas, distribuidas y actualizadas para que los empleados estén totalmente conscientes de las expectativas y responsabilidades. Por lo general, aquí es donde el analista de sistemas tendrá contacto por primera vez con aspectos de comportamiento de la seguridad.

Parte de la faceta de comportamiento de la seguridad es monitorear el comportamiento a intervalos irregulares para asegurarse de que se estén siguiendo los procedimientos adecuados y para corregir cualquier comportamiento que los haya erosionado con el tiempo. El hacer que el sistema registre la cantidad de intentos de registro no satisfactorios de los usuarios es una forma de monitorear si usuarios no autorizados están tratando de registrarse en el sistema. El inventario periódico y frecuente de equipo y software es deseable. Además, se deben examinar sesiones extrañamente largas o el acceso después de horas de trabajo no típico al sistema.

La salida generada por el sistema debe ser reconocida por su potencial de poner la organización en riesgo en algunas circunstancias. Los controles de la salida incluyen pantallas que sólo pueden ser accesadas por medio de contraseñas, clasificación de información (esto es, a quién se le puede distribuir y cuándo) y almacenamiento seguro de documentos impresos y almacenados magnéticamente.

En algunos casos se debe hacer provisiones para la destrucción de documentos que son clasificados o propios. Se pueden contratar servicios de destrucción o pulverización de una empresa externa, por una cuota, que destruirán medios magnéticos, cartuchos de máquinas de escribir e impresoras y papel.

2.7.3.4 Seguridad en las computadoras: Reducción de Riesgos. Para Beekman, (1995) la seguridad en las computadoras se ha convertido en una preocupación importante para los administradores de sistemas y usuarios. La seguridad en las computadoras consiste en proteger

los sistemas de computación y la información que ellos contienen contra el acceso, el daño, la modificación o la destrucción no autorizados. Las computadoras tienen dos características inherentes que los hacen vulnerables a ataques o errores operativos:

- Una computadora hará exactamente aquello para lo cual está programado, como revelar información confidencial. Cualquier sistema que pueda ser programado puede ser reprogramado por alguien que posea los conocimientos suficientes.
- Toda computadora únicamente puede hacer aquello para lo cual fue programado. "... no se puede proteger de averías o ataques liberados, a menos que esos casos hayan sido previstos, estudiados y atacados específicamente con una programación apropiada."

Quienes poseen o administran computadoras cuentan con una diversidad de técnicas de seguridad para proteger sus sistemas, desde las cerraduras ordinarias de baja tecnología hasta el ciframiento de software de alta tecnología.

Es muy importante tomarse en cuenta y tener conocimiento de los tipos de seguridad con los que una empresa puede y debe contar para evitar posibles riesgos en todo el equipo de cómputo.

2.7.3.5 Restricciones de acceso físico. Una forma de reducir el riesgo de violaciones a la seguridad consiste en asegurarse de que sólo el personal autorizado tenga acceso al equipo de cómputo, afirma Beekman, (1995). Las organizaciones usan varias herramientas y técnicas para identificar al personal autorizado. Algunas de estas revisiones de seguridad son efectuadas por la computadora; y otras por guardas de seguridad humanos. Dependiendo del sistema de seguridad, un usuario puede tener acceso a la computadora con base en:

- *Algo que tiene*: una llave, una tarjeta de identificación con fotografía o una tarjeta inteligente con una identificación codificada digitalmente;
- *Algo que sabe*: una contraseña, un número de identificación, la combinación de un candado o datos personales, como el nombre de su escritor preferido;
- *Algo que hace*: su firma o su velocidad para teclear y sus patrones de errores;
- *Algo acerca de usted*: su voz, huellas dactilares, lectura retinal u otras mediciones de las características corporales de un individuo, llamadas biométricas.

La seguridad es mucho más difícil en un ambiente en red, distribuido. No basta limitar el acceso físico a las macrocomputadoras cuando las computadoras personales y las conexiones de red no están restringidos. Para limitar el acceso a computadoras remotas se requieren de otras técnicas de seguridad, en especial las contraseñas.

2.7.3.6 Contraseñas. Según Beekman, (1995) las contraseñas son las herramientas más comunes para restringir el acceso a los sistemas de computación pero sólo serán eficaces si se eligen con cuidado. En su mayoría, los usuarios suelen elegir contraseñas que son fáciles de adivinar.

El software de control de acceso no tiene que tratar a todos los usuarios de la misma manera. En muchos sistemas se usan contraseñas para restringir a los usuarios de manera que sólo puedan abrir los archivos relacionados con su trabajo. En muchos casos, a los usuarios únicamente se les permite tener acceso de sólo lectura a los archivos, que pueden ver, pero no modificar.

Para evitar el uso no autorizado de contraseñas robadas por extraños, muchas compañías emplean sistemas de *devolución de llamada.* Cuando un usuario ingresa y teclea una contraseña, el sistema cuelga, busca el número telefónico del usuario y lo llama antes de permitir el acceso.

2.7.3.7 Respaldos. Ni siquiera el mejor sistema de seguridad puede garantizar la protección absoluta de los datos. El sabotaje, los errores humanos, las fallas de energía, las averías de máquina, los incendios, inundaciones, relámpagos y terremotos pueden dañar o destruir los datos de una computadora, con todo y hardware. Todo sistema de seguridad integral debe incluir algún tipo de plan para recuperarse de desastres. El seguro de recuperación de datos más eficaz y utilizado, tanto para macrocomputadoras como para computadoras personales, es un sistema para hacer respaldos regulares. En muchos sistemas, los datos y el software se respaldan automáticamente en discos, por lo general al final de cada jornada de trabajo. Muchos centros de procesamiento de datos mantienen varias generaciones de respaldos por que, dado el caso,

puedan retroceder varios días, semanas o años y reconstruir archivos de datos. Muchos usuarios de computadoras optan por un máximo de seguridad y mantienen copias de los datos importantes en varios lugares distintos.

2.8 El Informe de Auditoría.

Para Piatinni y Del Peso, (1998) la función de la auditoría se materializa exclusivamente por escrito. Por lo tanto la elaboración final es el exponente de su calidad. Para la realización del informe de auditoría se necesitan seguir ciertos pasos.

2.8.1 La evidencia. En esta parte se reseñan algunos asuntos previos, referidos a la redacción del informe, puesto que el referido informe es su consecuencia.

Por tanto, en qué consiste la evidencia en Auditoría Informática, así como las pruebas que la avalan, sin olvidar la importancia relativa y el riesgo probable, inherente y de control.

La certeza absoluta no siempre existe, según el punto de vista de los auditores; los usuarios piensan lo contrario. No obstante lo dicho, el desarrollo del control interno, incluso del específicamente informático, está en efervescencia, gracias al empuje de los informes.

Pero retomando la evidencia, se le considera la base razonable de la opinión del Auditor Informático. La evidencia tiene una serie de calificativos a saber:

- La **evidencia relevante**, que tiene una relación lógica con los objetivos de la Auditoría.
- La **evidencia fiable**, que es válida y objetiva, con nivel de confianza.
- La **evidencia suficiente**, que es de tipo cuantitativo para soportar la opinión profesional del auditor.
- La **evidencia adecuada**, que es de tipo cualitativo, afectando a las conclusiones del auditor.

En principio, las pruebas son de cumplimiento o sustantivas. La opinión deberá estar basada en evidencias justificativas, es decir, desprovistas de prejuicios, si es preciso con evidencia adicional.

2.8.2 La documentación. En el argot de Auditoría se conoce como papeles de trabajo la "totalidad de los documentos preparados o recibidos por el auditor, de manera que, en conjunto, constituyen un compendio de la información utilizada y de las pruebas efectuadas en la ejecución de su trabajo, junto con las decisiones que ha habido tomar para llegar a formarse su opinión".

El informe de Auditoría, si se precisa que sea profesional, tiene que estar basado en la documentación o papeles de trabajo, como utilidad inmediata, previa supervisión.

La documentación, además de fuente del Auditor Informático para trabajos posteriores así como para realizar su gestión interna de calidad, es fuente en algunos casos en los que la corporación profesional puede realizar un control de calidad, o hacerlo algún organismo oficial. Los papeles de trabajo pueden llegar a tener valor en los Tribunales de Justicia.

Por otra parte, no se debe omitir la característica registral del informe, tanto en su parte cronológica como en la organizativa, con procedimientos del archivo, búsqueda, custodia y conservación de su documentación, cumpliendo toda la normativa vigente, legal y profesional, como mínimo exigible. Los trabajos utilizados, en el curso de una labor, de otros auditores externos y/o expertos independientes, así como de los auditores internos, se reseñen o no en el Informe de Auditoría Informática, formarán parte de la documentación. Además, se incluirán:

- El contrato cliente/auditor informático y/o la carta propuesta del auditor informático.
- Las declaraciones de la Dirección.
- Los contratos, o equivalentes, que afecten al sistema de información, así como el informe de la asesoría jurídica del cliente sobre sus asuntos actuales y previsibles.
- El informe sobre terceros vinculados.
- Conocimientos de la actividad del cliente.

Estos son los aspectos que se deben tomar en cuenta para la realización del informe.

2.8.3 El informe. Para Piattini y Del Peso, (1998) se ha realizado una visión rápida de los aspectos previos para tenerlos muy presentes al redactar el Informe de Auditoría Informática, esto es, la comunicación del Auditor Informático al cliente, tanto del alcance de la Auditoría (objetivos, período de cobertura, naturaleza y extensión del trabajo realizado) como de los resultados y conclusiones.

Es momento adecuado de separar lo significativo de lo que no es significativo, debidamente evaluados por su importancia y vinculación con el factor riesgo, tarea eminentemente de carácter profesional y ético, según el leal saber y entender del Auditor Informático.

Aunque no existe un formato vinculante, sí existen esquemas recomendados con los requisitos mínimos aconsejables respecto a estructura y contenido.

También es cuestión previa decidir si el informe es largo o corto, por supuesto con otros informes sobre aspectos, bien más detallados, bien más concretos, como el informe de debilidades del control interno, incluso de hechos o aspectos; todo ello teniendo en cuenta la legislación vigente como el contrato con el cliente.

En lo referente a su redacción, el Informe deberá ser claro, adecuado, suficiente y comprensible. Una utilización apropiada del lenguaje informático resulta recomendable.

Los puntos esenciales, genéricos y mínimos del Informe de Auditoría Informática son los siguientes:

1) Identificación del Informe. El título del informe deberá identificarse con objeto de distinguirlo de otros informes.

2) Identificación del Cliente. Deberá identificarse a los destinatarios y a las personas que efectúen el encargo.

3) Identificación de la entidad auditada. Identificación de la entidad objeto de la Auditoría Informática.

4) Objetivos de la Auditoría Informática. Declaración de los objetivos de la Auditoría para identificar su propósito, señalando los objetivos incumplidos.

5) Normativa aplicada y excepciones. Identificación de las normas legales y profesionales utilizadas, así como las excepciones significativas de uso y el posible impacto en los resultados de Auditoría.

6) Alcance de la Auditoría. Concretar la naturaleza y extensión del trabajo realizado: área organizativa, período de Auditoría, sistemas de información, señalando limitaciones del alcance y restricciones del auditado.

7) Conclusiones: Informe corto de opinión. Lógicamente, se ha llegado a los resultados y, sobre todo, a la esencia del dictamen, la opinión y los párrafos de salvedades y énfasis, si procede.

El informe debe contener uno de los siguientes tipos de opinión: **favorable o sin salvedades, con salvedades, desfavorable o adversa, y denegada**.

Opinión favorable. La opinión calificada como favorable, sin salvedades o limpia, deberá manifestarse de forma clara y precisa, y es el resultado de un trabajo realizado sin limitaciones de alcance y sin incertidumbre, de acuerdo con la normativa legal y profesional.

Es indudable que entre el informe de recomendaciones al cliente, que incluye lo referente a debilidades de control interno en sentido amplio, y las salvedades, existe o puede existir una zona de gran sensibilidad; tan es así que tendrá que clarificarse al máximo, pues una salvedad a la opinión deberá ser realmente significativa; concretando: ni pasarse, ni no llegar, dicho en lenguaje coloquial; en puridad es un punto de no retorno.

Opinión con salvedades. Se reitera lo dicho en la opinión favorable al respecto de las salvedades cuando sean significativas en relación con los objetivos de Auditoría, describiéndose con precisión la naturaleza y razones.

Podrían ser éstas, según las circunstancias, las siguientes:

- ♣ Limitaciones al alcance del trabajo realizado; esto es, restricciones por parte del auditado, etc.
- ♣ Incertidumbres cuyo resultado no permita una previsión razonable.
- ♣ Irregularidades significativas.
- ♣ Incumplimiento de la normativa legal y profesional.

Opinión desfavorable. La opinión desfavorable o adversa es aplicable en el caso de:

- ♣ Identificación de irregularidades
- ♣ Incumplimiento de la normativa legal y profesional, que afecten significativamente a los objetivos de Auditoría informática estipulados, incluso con incertidumbres; todo ello en la evaluación de conjunto y reseñando detalladamente las razones correspondientes.

Opinión denegada. La denegación de opinión puede tener su origen en:

- ♣ Las limitaciones al alcance de Auditoría.
- ♣ Incertidumbres significativas de un modo tal que impidan al auditor formarse.
- ♣ Irregularidades.
- ♣ El incumplimiento de normativa legal y profesional.

Resumen. El siempre difícil tema de la opinión, estrella del Informe de Auditoría Informática, joven como informática y más todavía como Auditoría informática; por tanto, puede decirse que más cambiante. Debido a ello, y además con la normativa legal y profesional desacompasadas, la ética se convierte casi en la única fuente de orientación para reducir el desfase entre las expectativas del usuario en general y el informe de los auditores.

8) Resultados: Informe largo y otros informes. Parece ser que, de acuerdo con la teoría de los ciclos, el informe largo va a colocar al informe corto en su debido en su sitio, o sea, como resumen del informe largo (¿quizá obsoleto?). Los usuarios, no hay duda, desean saber más y desean transparencia como valor añadido.

Es indudable que el límite lo marcan los papeles de trabajo o documentación de la Auditoría Informática, pero existen aspectos a tener en cuenta:

- ♣ El secreto de la empresa.
- ♣ El secreto profesional.
- ♣ Los aspectos relevantes de la Auditoría.

Las soluciones previsibles se orientan hacia un informe por cada objetivo de la Auditoría Informática, como los informes especiales y/o complementarios que exigen algunos organismos gubernamentales.

9) Informes previos. No es una práctica recomendable, aunque sí usual en algunos casos, ya que el Informe de Auditoría Informática es, por principio, un **informe de conjunto**.

Sin embargo, en el caso de detección de irregularidades significativas, tanto errores como fraudes, sobre todo, se requiere una actuación inmediata según la normativa legal y profesional, independientemente del nivel jerárquico afectado dentro de la estructura de la entidad.

10) Fecha del informe. El tiempo no es neutral; la fecha del Informe es importante, no sólo por la cuantificación de honorarios y el cumplimiento con el cliente, sino para conocer la magnitud del trabajo y sus implicaciones. Conviene precisar las fechas de inicio y conclusión del trabajo de campo, incluso la del cierre de ejercicio, si es que se está realizando un Informe de Auditoría Informática como herramienta de apoyo a la Auditoría de Cuentas. En casos

conflictivos pueden ser relevantes los aspectos tales como hechos posteriores al fin del período de Auditoría, hechos anteriores y posteriores al trabajo de campo.

11) Identificación y firma del auditor. Este aspecto formal del informe es esencial tanto si es individual como si forma parte de una sociedad de Auditoría, que deberá corresponder a un socio o socios legalmente así considerados.

12) Distribución del informe. Bien en el contrato, bien en la carta de propuesta del Auditor Informático, deberá definirse quién o quiénes podrán hacer uso del Informe, así como los usos concretos que tendrá, pues los honorarios deberán guardar relación con la responsabilidad civil.

El auditor debe redactar el informe final de manera clara y exacta siguiendo el proceso de elaboración de un informe de auditoría informática.

2.9 Los Contratos Informáticos.

El contrato informático, según Piatinni y Del Peso, (1998). "Es aquel cuyo objeto es un bien o un servicio informático –o ambos- o que una de las prestaciones de la parte tenga por objeto ese bien o servicio informático".

Los contratos informáticos se suelen dividir en cuatro grandes grupos: hardware, software, servicios y complejos.

Se entiende que esta división no responde ya a la realidad, y para una mayor clarificación del problema y una mayor homogeneidad esta clasificación se debe ampliar del siguiente modo:

- ***Contratación del hardware.-*** El objeto de la contratación en esta clase de contratos es el hardware, o sea, la parte física del ordenador y de sus equipos auxiliares. Este tipo de contratos no suelen presentar problemas específicos. Los contratos más usuales son los siguientes:
    1) Compraventa
    2) Arrendamiento
    3) Arrendamiento financiero (leasing)

4) Mantenimiento

- ***Contratación del software.-*** Los contratos más corrientes son los siguientes:
  1) ***Desarrollo del software.-*** Se trata del caso en que una persona física, un colectivo o una empresa crean un software específico, a medida para otro. El tipo de contrato puede ser: arrendamiento de servicios o de obra, mercantil o laboral.
  2) ***Licencia de uso.***- Es el contrato en virtud del cual el titular de los derechos de explotación de un programa de ordenador autoriza a otro a utilizar el programa, conservando el cedente la propiedad del mismo. Esta autorización, salvo pacto en contrario, se entiende de carácter no exclusivo e intransferible.
  3) ***Adaptación de un software producto.***- Se trata de la contratación de una licencia de uso de un producto estándar que habrá de adaptar a las necesidades del usuario.
  4) ***Mantenimiento.***- El contrato de mantenimiento en un principio tiene por objeto corregir cualquier error detectado en los programas fuera del período de garantía. Se consideran varios tipos de mantenimiento: Correctivo, de adaptación, perfectivo y preventivo.
  5) ***Garantía de acceso al código fuente.-*** Es aquel que tiene por objeto garantizar al usuario el acceso a un programa fuente en el caso de que desaparezca la empresa titular de los derechos de propiedad intelectual. Consiste en el depósito del programa fuente en un fedatario público, que lo custodia, por si en el futuro es preciso acceder al mismo.
- ***Contratación de servicios.-*** Los contratos de servicios informáticos más importantes son los siguientes:
  1) ***Consultoría informática***
  2) ***Auditoría informática***
  3) ***Formación***
  4) ***Seguridad Informática***
  5) ***Contratación del personal informático***
  6) ***Instalación***
  7) ***Comunicaciones***

8) ***Seguros***
9) ***Responsabilidad Civil.***

♣ ***Contratos complejos.-*** Son aquellos que contemplan los sistemas informáticos como un todo incorporando al objeto del mismo, tanto el hardware como el software y algunos servicios determinados. Los más usuales son los siguientes:

1) ***Contratación global o parcial de servicios informáticos (Outsourcing).-*** Se trata de la subcontratación de todo o de parte del trabajo informático mediante un contrato con una empresa externa que se integra en la estrategia de la empresa y busca diseñar una solución a los problemas existentes.
2) ***Contrato de respaldo (Back up).-*** Su finalidad es asegurar el mantenimiento de la actividad empresarial en el caso de que circunstancias previstas pero inevitables impidan que siga funcionando el sistema informático.
3) ***Contrato de llave en mano (turn-key-package***).- En esta clase de contratos el proveedor se compromete a entregar el sistema creado donde el cliente le indique y asume la responsabilidad total de diseño, realización, pruebas, integración y adaptación al entorno ofimático del cliente tanto lógico como físico.
4) ***Contrato de suministro de energía informática.-*** "Aquel mediante el que una parte –el suministrador- poseedor de una unidad central que permanece en sus locales, pone a disposición del usuario la misma, lo que le permite el acceso a los "software", a cambio de un precio".

Dependiendo las necesidades de la empresa, se debe contar con distintos contratos informáticos donde se avalen ciertos servicios a equipos de cómputo.

2.10 Los Delitos Informáticos.

Según Piattini y Del Peso, (1998) fraude puede ser definido como engaño, acción contraria a la verdad o a la rectitud. La definición de delito puede ser más compleja.

Muchos estudios del Derecho Penal han intentado formular una noción de delito que sirviese para todos los tiempos y en todos los países. Esto no ha sido posible dada la íntima conexión que existe entre la vida social y la jurídica de cada pueblo y cada siglo, aquella condiciona a ésta.

Los elementos integrantes del delito son:

1) El delito es un acto humano, es una acción (acción u omisión)
2) Dicho acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.
3) Debe corresponder a un tipo legal (figura del delito), definido por la ley, ha de ser un acto típico.
4) El acto de ser culpable, imputable a dolo (intención) o a la culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.
5) La ejecución u omisión del acto debe estar sancionada con una pena.

Por tanto, un delito es: una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado con una pena.

Se podría definir el delito informático como toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la ley, que se realiza en el entorno informático y está sancionado con una pena.

Contemplando el delito informático en un sentido amplio se pueden formar varios grandes grupos de figuras delictivas claramente diferenciadas:

1) Delitos contra la intimidad

- ♣ Apoderación de mensajes electrónicos u otros documentos.
- ♣ Interceptación de comunicaciones
- ♣ Utilización de artificios técnicos de escucha, transmisión, grabación o reproducción de sonido, imagen o cualquier otra señal de documentación.
- ♣ Apoderación y en perjuicio de terceros datos reservados de carácter personal o familiar que se hallen en archivos o soportes informáticos.

- ♣ Los delitos son agravantes si se dan en función de: Carácter de datos (religión, salud, vida sexual, origen racial) y las circunstancias de la víctima (menor de edad o incapaz).

2) ***Delitos contra el patrimonio.-*** Entre los delitos contra el patrimonio se encuentran: la estafa informática, las defraudaciones, los daños informáticos y la propiedad intelectual.

   a) Estafa Informática.- Los que con ánimo de lucro, y valiéndose de alguna manipulación informática consiga la transferencia no consentida de cualquier activo patrimonial en perjuicio a un tercero.

   b) Defraudaciones.- Es el uso, sin consentimiento de su titular de cualquier equipo terminal de telecomunicación.

   c) Daños informáticos.- Al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos. Entre estas situaciones se pueden incluir los famosos virus informáticos, bombas lógicas y hackers.

   d) Propiedad intelectual.- Es la reproducción, plagio, distribución o comunicación pública con fines de lucro en todo o en parte de una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

   La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.

   Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

3) ***Falsedades documentales.-*** Se refiere a la falsificación y puesta en circulación de cualquier documento (todo material que exprese o incorpore datos).

Todos estos delitos pueden repercutir significativamente a la empresa en caso de descubrirse, ocasionando pérdidas tanto económicas como legales.

2.11 Definición de Sistemas de Información.

Según Cohen, (1996) un sistema de información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de la empresa o negocio.

En un sentido amplio se puede considerar un Sistema de Información (SI) como un conjunto de componentes que interactúan para que la empresa pueda alcanzar sus objetivos satisfactoriamente.

2.12 Aplicaciones para equipo de cómputo.

Según Beekman, (1995), los programas de aplicación, o aplicaciones son las herramientas de software que permiten usar una computadora para fines específicos. Muchas de las aplicaciones en los terrenos científico, gubernamental, administrativo y artístico son tan especializadas y técnicas que no son de utilidad o interés para quienes no se ocupan de esos campos. Por otra parte, algunas aplicaciones son tan flexibles que pueden servir a casi cualquier persona.

Algunas aplicaciones son las siguientes:

Visual Basic 6.0 es la herramienta más productiva para crear aplicaciones de alto rendimiento empresariales y basadas en Web. Es utilizado por desarrolladores de sistemas.

Microsoft Office 97 para la pequeña y mediana empresa (PYME) es el conjunto de programas de oficina que integra aplicaciones inteligentes que aumentan la productividad con la

capacidad de Internet para ayudar a las personas de las pequeñas organizaciones a realizar su trabajo de forma mejor y nueva.

Microsoft® SQL Server™ versión 7.0 es una versión decisiva dentro de los productos de bases de datos de Microsoft, que se basa en los sólidos cimientos establecidos por SQL Server versión 6.5. Como la base de datos mas sólida de la familia Windows, SQL Server es el sistema de administración de bases de datos relacionales (RDBMS) más conveniente para una amplia gama de usuarios corporativos y proveedores independientes de software (ISV) que generan aplicaciones comerciales. Las necesidades y requisitos de los clientes han llevado a significativas innovaciones en el producto en facilidad de uso, confiabilidad y escalabilidad, y en almacenes de datos.

El sistema operativo **Microsoft Windows 98** es la actualización de Windows que hace que el equipo trabaje y funcione mejor. Trabaja mejor al hacer que el acceso a Internet sea más sencillo y al proporcionar mejor rendimiento del sistema, todo ello junto con diagnósticos y mantenimiento del sistema más sencillos. Con Windows 98, el sistema también funciona mejor ya que es compatible con las tecnologías más avanzadas de gráficos, sonido y multimedia, cuenta con la capacidad de agregar y quitar dispositivos periféricos con compatibilidad con el Bus serie universal (USB) y permite la convergencia del equipo personal y de la TV en su hogar. Este nuevo y atractivo sistema operativo está construido sobre las innovadoras características presentadas en Windows 95. Al mismo tiempo, Windows 98 mantiene la mejor compatibilidad con las antiguas aplicaciones y tecnologías basadas en Windows.

Windows 2000. El sistema operativo para equipos portátiles y de escritorio ideal para todo tipo de empresas. Basado en la tecnología de NT, Windows 2000 Professional ofrece una confiabilidad muy sólida y características mejoradas de administración que simplifican la administración del escritorio. Además, al integrar capacidades Web y amplia compatibilidad con equipos móviles y dispositivos de hardware, facilita a los usuarios de empresas conectarse a Internet y trabajar en cualquier lugar y a cualquier hora.

Wingate es una aplicación que permite que a través de una sola conexión puedan acceder a Internet varios usuarios de una misma red local, todos ellos al mismo tiempo y sin interferirse unos a otros.

Corel Draw es el más completo programa de diseño gráfico e ilustración, este programa trae rápidas herramientas de ilustración, contiene efectos especiales fáciles de usar, que lo

convierten en el programa ideal para la creación de cualquier proyecto de diseño. Con Corel Draw podrá realizarse infinidad de piezas publicitarias, logotipos, empaques, etc.

Sygate permite compartir una única conexión a Internet con varias computadoras que integren la red por medio de un Firewall de protección. Entre sus características se destacan, por ejemplo, la facilidad de uso, la posibilidad de especificar que maquina navegará con mayor prioridad, opciones para especificar filtros especiales y más.

ICQ es un programa de mensajes instantáneos ICQ ("I seek you"), el cual permite comunicarse con amigos y colegas en tiempo real.

Yahoo Messenger permite hacer uso del servicio gratuito que ofrece Yahoo, permitiendo ver a amigos cuando se encuentran en línea para enviarles mensajes instantáneos e intercambiar opiniones con tus amigos

Outlook Express es un programa que permite recibir y enviar correo electrónico (e-mail) desde cualquier computadora.

Norton Antivirus es un programa que permite proteger los virus, evitando su intrusión al sistema.

Todas las aplicaciones son de gran ayuda dentro de una organización, porque permiten agilizar procesos, mejorar la comunicación, realizar mejores trabajos así como proteger su información de los virus.

2.13 Licencias para el uso de aplicaciones.

Para Beekman, (1995) al comprar un paquete corriente de software, en realidad no está comprando el software, sino una licencia de software que le permite usar el programa en la máquina. Los acuerdos de licencia varían de una compañía a otra, pero la mayoría incluye limitaciones en cuanto al derecho del usuario a copiar discos, instalar software en discos duros y transferir información a otros usuarios. Casi todos los productos de software comercial en el mercado tienen derechos de autor, de modo que no pueden duplicarse legalmente para ser distribuidos a terceros; algunos discos están protegidos contra copias, de manera física, para que

no puedan copiarse. La creación de software es increíblemente costosa, debido a su dificultad. La mayoría de los creadores de software usan los derechos de autor y la protección contra copias para asegurarse de que vendan suficientes copias de sus productos para recuperar su inversión seguir operando y escribir más programas.

2.14 Virus informáticos.

Según Levin, (1992) los virus informáticos son programas de software del mismo modo que los procesadores de textos, hojas de cálculo, gestores de bases de datos, etc., son programas informáticos. Esto significa que son simplemente listas de instrucciones que dicen a las computadoras qué acciones hay que ejecutar y precisamente cómo ejecutarlas. Los virus informáticos pueden, por tanto, realizar todas las operaciones que sean soportadas por el sistema operativo de la computadora principal, al igual que cualquier otro componente de software puede realizar esas operaciones.

Los virus se cargan y se ejecutan sin autorización de los usuarios; se esconden dentro de los programas normales (llamados programas centrales) y son realizados cuando se ejecutan los programas centrales. Los virus actúan sin pedir permiso a los usuarios y sin avisarles de las consecuencias de sus acciones.

Los virus pueden formatear discos, copiar, renombrar y borrar archivos, reproducirse con nueva información de configuración, modificar fechas y características de archivos, llamar a otras computadoras para telecargar archivos, etc. Si la acción puede ser realizada por software informático puede ser realizada por un virus informático.

2.15 Mantenimiento.

Para Mueller, (1999) el mantenimiento es otro de los factores cruciales a tomar en cuenta durante la evaluación técnica de las propuestas. Consiste básicamente en la capacidad de un

proveedor para proporcionar un soporte y servicio adecuado, para asegurar el funcionamiento continuo e ininterrumpido del sistema computacional. Algunos de los aspectos a considerar son los siguientes:

- Calidad y cantidad de personal capacitado de tiempo completo disponible en hardware y software.
- Tiempo promedio que tarda el proveedor en atender las fallas reportadas.
- Tiempo o porcentaje de sistema funcionando, que es el tiempo que dura trabajando el sistema sin que ocurra algún problema.
- Tiempo promedio que el sistema permanece caído durante cada falla.
- Horario de soportes.

Según Piattini y Del Peso, (1998) el contrato de mantenimiento, en principio tiene por objeto corregir cualquier error detectado en los programas fuera del período de garantía. Se consideran varios tipos de mantenimiento: Correctivo, de adaptación, perfectivo y preventivo.

2.15.1 <u>Tipos de mantenimiento.</u> El mantenimiento puede dividirse en tres tipos:

- ♣ Preventivos

Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones.

- ♣ Detectivos

Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. Son los más importantes para el auditor. En cierta forma sirven para evaluar la eficiencia de los controles preventivos.

- ♣ Correctivos

Ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en si una actividad altamente propensa a errores.

2.18 Garantías de equipo de cómputo.

Según Mueller, (1999) las garantías son una tendencia más bien reciente en la industria de la computación. En la actualidad, el otorgar una buena garantía sobre sus productos, es una forma en que los vendedores logran sobresalir de entre la multitud de feroces competidores. La mayoría de las compañías ofrecen una garantía de un año en sus sistemas, pero otras ofrecen períodos mayores, que incluyen tres años o más.

Al tener conocimiento de todos los conceptos a utilizar en este estudio, se podrá comprender claramente el contenido de toda la investigación.

CAPÍTULO III

METODOLOGÍA

Según Piattini y Del Peso, (1998) la evolución sufrida en el entorno microinformático ha condicionado el desarrollo de los sistemas ofimáticos actuales. El aumento de la potencia del cálculo, la reducción de costos de los ordenadores personales y las estaciones de trabajo, ha desplazado el desarrollo de aplicaciones ofimáticas a formas microinformáticas y redes de área local.

Como consecuencia de los grandes adelantos tecnológicos, la situación actual de los sistemas de información en los negocios se caracteriza por una falta de asimilación de las nuevas tecnologías, obsolescencia en los sistemas, falta de planificación, abundante piratería, y delitos informáticos, que están proliferando cada día más entre los sistemas, en sí por una falta de estándares, metodologías e información; sobre todo en los aspectos de control y seguridad informática.

Es por ello, que es de suma importancia dar a conocer a las empresas la manera correcta para trabajar y explicarles el por qué la situación ha cambiado y ayudarles a mejorar y aprovechar mejor todos los recursos que tienen a su alcance.

La metodología sugerida pretende dar a conocer a la empresa las fallas que están teniendo y la forma de solucionarlas; para lograr tener eficacia y eficiencia en sus procesos.

3.1 Sujetos.

El presente estudio se realizó en el período comprendido del 21 de Agosto al 13 de Octubre del 2000, en la empresa "La Casita" dedicada a la construcción de fraccionamientos y viviendas, la cual se encuentra ubicada en Cd. Obregón, Sonora, y cuenta actualmente con varias sucursales dentro del Estado. Esta empresa se considera bastante sólida y con características bien definidas. En la actualidad trabaja con personal altamente capacitado y utiliza tecnología de punta, lo cual hace que tenga un nivel competitivo en el mercado. "La Casita" cuenta con varios departamentos que se muestran en el Anexo 1.

Para realizar el desarrollo de la Auditoría Ofimática se realizó una encuesta dirigida al departamento de Sistemas de la empresa "La Casita", que son los que conocen los equipos de cómputo y aplicaciones de la organización, específicamente a los encargados de él, pero en sí, este departamento está conformado por: El Administrador de la Red, Jefe de Desarrollo de Sistemas y dos programadores analistas.

Las dos personas entrevistadas fueron los primeros mencionados y tienen suficientes conocimientos sobre Sistemas de Información y Redes, el puesto que desempeñan actualmente se obtuvo por medio de la entrevista (Apéndice A) y se describe a continuación:

Administrador de la Red: Es el responsable de mantener en línea los servicios de la red en función de los horarios establecidos para cada tipo de servicios. Además, es el responsable de coordinar la instalación y cambios físicos de equipo de cómputo, líneas de comunicación y terminales, garantizando que reúnan los requerimientos confiables de seguridad para evitar accidentes o fallas constantes. También se le otorgó la responsabilidad de realizar la compra de equipos de cómputo y de aplicaciones; todo lo realiza para el noroeste de la República Mexicana.

Jefe de Desarrollo de Sistemas: Es el responsable de automatizar los requerimientos de los usuarios que por el alcance de sus operaciones dentro de la institución, volúmenes de datos y requerimientos específicos de servicio, necesitan ser satisfechos mediante el desarrollo de sistemas, o el aprovechamiento de las bases de datos en el servidor principal.

3.2 Materiales.

Para la aplicación de la Auditoría Ofimática se realizaron diversas formas para recabar datos; como entrevistas, cuestionarios, observaciones, revisión de la documentación y computadoras, formatos utilizados. Una vez obtenida la información que se necesita, se procede a analizarla para obtener resultados que ayudan para la realización del informe de auditoría.

Todas las formas que se utilizaron para la obtención de datos son muy importantes para esta auditoría, destacando entre ellas la aplicación del cuestionario.

El cuestionario fue realizado por los autores de este trabajo, basándose en fundamentos teóricos sobre la Auditoría Ofimática según Piattini y Del Peso, (1998) auditoría que está dividida en las siguientes partes: Economía, Eficiencia, Eficacia y Seguridad. El cuestionario se dividió en las partes antes mencionadas para su mejor comprensión y facilidad de uso, obteniendo un total de 99 preguntas abiertas relacionadas con el tema y validadas por la participación de un experto, mostradas en el Apéndice B. Éstas se realizaron abiertas porque se necesitaban respuestas detalladas y precisas.

El método utilizado para la aplicación del cuestionario es por medio de preguntas a los encuestados, y el tiempo requerido para la aplicación de él puede variar dependiendo el tiempo disponible de los entrevistados, puede llegar a requerir de un día entero.

3.3 Procedimiento.

El procedimiento utilizado para realizar el estudio, se describe a continuación: Primeramente, se solicitó a la empresa “La Casita”, la posibilidad de aplicar la Auditoría Ofimática, ya que no en todas las empresas de la localidad puede ser aplicada debido a que en la mayoría de ellas, el departamento de Sistemas es dirigido desde otra localidad o muchas no cuentan con ese departamento.

Una vez que el estudio fue aceptado por la empresa, se procedió a definir los días en que podría aplicarse la auditoría, dando como resultado un programa de varios días en los que se realizarían las entrevistas, se aplicaría el cuestionario y la revisión de la documentación existente para obtener la información necesaria.

Posteriormente se realizaron las entrevistas (Apéndice A) con los encargados del Departamento de Sistemas, conociendo sus puestos: Administrador de Red y Jefe de Desarrollo de Sistemas, también se dio un recorrido por la empresa para conocer mejor su funcionamiento, se realizó la aplicación del cuestionario a los encargados del Departamento de Sistemas, y por último, se realizó la revisión de papeles de trabajo, documentación de aplicaciones y formatos utilizados.

Durante los días en los que se llevó a cabo la auditoría se observaron y revisaron las computadoras para corroborar que la información que proporcionaban era correcta y verídica.

Finalmente, una vez aplicado el cuestionario (Apéndice B), se procedió a analizar e interpretar los resultados obtenidos, los cuales proporcionan la información necesaria para elaborar el informe final y dar a la empresa sugerencias y recomendaciones, que pudieran ser de gran utilidad para mejorar el funcionamiento de la empresa.

El objeto primordial de este capítulo fue proporcionar información detallada acerca de la forma en que se realizó el estudio.

CAPÍTULO IV

RESULTADOS Y DISCUSIONES

En la actualidad, se debe estar informado sobre la tecnología cambiante para estar al tanto de las mejoras que le puede traer al negocio al momento de adquirirla. Es por esto que también se debe tener control de las adquisiciones que se obtienen, así como el estar enterados de las implicaciones que éstas ocasionen.

La auditoria Ofimática es un término poco conocido por las empresas y es por ello que no se lleva a cabo en las organizaciones de una forma correcta

Si las empresas realizaran la Auditoría de la Ofimática dentro de su organización de una forma regular, podrían estar mejor enteradas de cómo está funcionando su oficina, saber si su inventario de cómputo y sus aplicaciones están siendo utilizados de una manera eficaz y eficiente, saber si se está siguiendo un buen procedimiento para la adquisición de nuevos productos, y conocer si la seguridad que se utiliza es la más adecuada.

En el presente capítulo se describen los resultados obtenidos de la Auditoría de la Ofimática realizada en la empresa “La Casita”, la información obtenida fue a través de entrevistas y cuestionarios donde se pudo obtener información más clara y verificándola por medio de la observación, donde además se solicitó documentación importante para la elaboración de este trabajo.

Al final de este capítulo, se observará de una forma más detallada el funcionamiento de la organización auditada, los resultados que se obtuvieron y comentarios que se obtuvieron.

4.1 Resultados.

Como ya se había mencionado, el objetivo general de esta investigación tiene el fin de proporcionar las herramientas necesarias para que una organización pueda aprovechar al máximo todas sus aplicaciones ofimáticas y tenga una mejor distribución de información en los diferentes departamentos, es por ello que se manejaron los criterios de seguridad, eficiencia en el manejo de la información, eficacia en los procesos para llevar a cabo la Auditoría ofimática, según Piattini y Del Peso, (1998).

Una vez obtenida la información de la Auditoría Ofimática en la empresa “La Casita” y de acuerdo a los resultados obtenidos se realizó el informe de auditoría emitiendo su correspondiente opinión que a continuación se presenta:

EL INFORME

1. ***Identificación del Informe***

AUDITORÍA OFIMÁTICA REALIZADA EN LA EMPRESA “LA CASITA”

2. ***Identificación del Cliente***

Por razones de fuerza mayor el nombre real de la empresa ha sido cambiado para la elaboración de esta investigación pero ésta puede identificarse como una mediana empresa, con solvencia económica y de competencia en el mercado.

3. Identificación de la entidad Auditada

En la empresa "La Casita" dedicada a la construcción de fraccionamientos y viviendas, la cual se encuentra ubicada en Ciudad Obregón, Sonora se realizó esta Auditoría Ofimática obteniendo el respectivo informe.

4. Objetivos de la Auditoría de la Ofimática

A continuación se señalan los objetivos de la Auditoría Ofimática:

- ♣ Determinar si el inventario ofimático refleja con exactitud los equipos y aplicaciones existentes en la organización.
- ♣ Determinar y evaluar el procedimiento de adquisiciones de equipos y aplicaciones.
- ♣ Determinar y evaluar la política de mantenimiento definida en la organización.
- ♣ Evaluar la calidad de las aplicaciones del entorno ofimático desarrollada por personal de la propia organización.
- ♣ Evaluar la corrección del procedimiento existente para la realización de los cambios de versiones y aplicaciones.
- ♣ Determinar si los usuarios cuentan con suficiente formación y la documentación de apoyo necesaria para desarrollar sus tareas de un modo eficiente.
- ♣ Determinar si el sistema existente se ajusta a las necesidades reales de la organización.
- ♣ Determinar si existen garantías suficientes para proteger los accesos no autorizados a la información reservada de la empresa y la integridad de la información.
- ♣ Determinar si el procedimiento de generación de copias de respaldo es fiable y garantiza la recuperación de la información en caso de necesidad.
- ♣ Determinar si está garantizado el funcionamiento ininterrumpido de aquellas aplicaciones cuya caída podría suponer pérdidas de integridad de la información y aplicaciones.
- ♣ Determinar el grado de exposición ante la posibilidad de intrusión de virus.
- ♣ Determinar si en el entorno ofimático se producen situaciones que pueden provocar infracciones**.**

5. Alcance de la Auditoría

El alcance que tuvo la Auditoría Ofimática realizada en la empresa "La Casita" en el Departamento de Sistemas y al haber aplicando un cuestionario al Administrador de la Red y al Jefe de Desarrollo de Sistemas, fue dentro del período de Agosto a Octubre del 2000 donde se tuvieron como limitaciones: la restricción del nombre real de la empresa y en algunas ocasiones no contaban con gran disponibilidad de tiempo retrasando un poco la investigación; sin embargo éstas no afectaron para la realización de esta investigación ni la elaboración del informe correspondiente. Para la revisión de la documentación (ordenes de compra, inventario de cómputo, solicitud de servicio, inventario contable), equipos y aplicaciones, no se tuvieron problemas debido a que se les permitió el acceso a los auditores de este trabajo.

6. Conclusiones

Como conclusión del informe basándose en los resultados correspondientes se dictaminó que el resultado es ***opinión con salvedades*** debido al incumplimiento de la normativa legal al no contar con las licencias correspondientes a aplicaciones que se utilizan dentro de la organización, este resultado no repercute a la empresa en su funcionamiento a menos que se les realizara una auditoría por parte de los creadores de software en donde se les pida comprobar las licencias de las aplicaciones, debiendo pagar la multa por cada computadora donde se encuentre el programa.

7. Detalles del informe

A continuación se encuentran los detalles del informe de cada objetivo que se trató en esta Auditoría:

Determinar si el inventario ofimático refleja con exactitud los equipos y aplicaciones existentes en la organización.

Se comprobó que sí se tiene un formato estructurado para garantizar que todos los equipos adquiridos en la organización son debidamente inventariados (Ver Anexo 3,4,5,6 y 7). El inventario se actualiza cada vez que se realiza alguna compra de equipo o producto.

Los datos que se registran en el inventario son:

- ♣ Equipo o Dispositivo
- ♣ Modelo

- ♣ Usuario
- ♣ Memoria
- ♣ Módem
- ♣ Red
- ♣ Cd-Rom
- ♣ Número de Control
- ♣ Departamento
- ♣ Plaza

El inventario es fiable debido a que se comprobó su autenticidad al compararlo con el inventario contable de la empresa (Anexo 9). La persona encargada de controlar este inventario es el Administrador de la Red.

Determinar y evaluar el procedimiento de adquisiciones de equipos y aplicaciones.

La empresa cuenta con una política de adquisiciones centralizada en la que en el departamento de sistemas es el encargado de realizar las compras de equipo de cómputo y aplicaciones.

Se comprobó que se valoran aspectos relativos a la necesidad real de los equipos solicitados, evaluando si lo que solicitan es realmente necesario, preguntándole al departamento solicitante: ¿Qué ocupan?¿ Para qué lo ocupan? ¿Cuánto lo ocupan? Y posteriormente se le hace una propuesta de equipo o producto que mejor se adapte a sus necesidades, si es que es aceptado.

En la empresa no realizan compra de paquetes o de contratos externos, solamente realizan compras para equipo de comunicaciones.

El procedimiento que se sigue para la autorización de compra dentro de la organización es:

1. Se recibe la requisición de una orden de compra (Ver Anexo 2).
2. Se cotiza con varios proveedores
3. Se analiza a los proveedores seleccionando al que cumpla con las características de un buen servicio, entrega rápida, garantía ofrecida, bajo costo, descuentos, marca del producto ofrecido, calidad del producto. (En la empresa casi siempre se tiene un mismo proveedor, el cual fue seleccionado por las características anteriores. En caso de necesitar algo que este proveedor no tenga, se vuelve a hacer un análisis de los proveedores)

4. Se realiza la orden de compra en el departamento de sistemas y la persona encargada de hacer las compras es el Administrador de Red.
5. La orden de compra debe ser autorizada por el Director General y el Gerente General, además del Administrador de la Red.

Determinar y evaluar la política de mantenimiento definido en la adquisición.

No existe una política de mantenimiento bien definida, más bien el mantenimiento es realizado por el Administrador de la Red, éste hace recorridos y cuando se observa que algún equipo le hace falta el servicio se le da. . El equipo se está utilizando constantemente, es por ello que se aprovecha cuando se desocupa alguno de ellos y se le da el mantenimiento correspondiente y se verifican las aplicaciones para ver si alguna de ellas no impide el buen funcionamiento del mismo. No manejan fechas o días específicos, éste se lleva a cabo cada vez que se puede.

En la empresa “La Casita” no cuentan con contratos de mantenimiento, pero si utilizan las garantías de los productos adquiridos en cuestión de disco duro y tarjetas de red solamente. También se conoce el estado de las garantías de cada uno de los productos, las cuales casi siempre son de un año y conocen el mecanismo para hacerla efectiva y el que ellos utilizan son la copia de la factura y el equipo.

En el momento en que la garantía caduca, la empresa ya se hace responsable del producto. También se conocen los productos en los que la responsabilidad del mantenimiento recae en la propia empresa.

No existen contrataciones con empresas externas para el mantenimiento pero sí existe una persona encargada de realizarlo en toda la zona noroeste y se encuentra en la sucursal matriz localizada en Cd. Obregón siendo éste el Administrador de la Red, quien es el que recibe la capacitación sobre los nuevos productos instalados.

En relación con la gestión de incidencias producidas, la empresa no cuenta con la existencia de un registro de las mismas, por lo tanto tampoco cuenta con un procedimiento establecido para asignar recursos para solucionarlas. Sin embargo, al ocurrir alguna incidencia el departamento de sistemas es el encargado de solucionarlo y el tiempo utilizado puede llegar a afectar el buen funcionamiento de la organización, porque si el problema es en Cd. Obregón se atiende al instante y el tiempo de solucionarlo es dependiendo de la incidencia ocurrida; en

cambio si el problema es fuera de la ciudad el tiempo de atención es mayor de un día como mínimo, ya que la persona encargada de solucionarlo tiene que ir a la ciudad donde ocurrió la incidencia.

Evaluar la calidad de las aplicaciones del entorno ofimático desarrollado por personal de la propia organización.

En la empresa "La Casita" existe un responsable de controlar el desarrollo de aplicaciones de toda la organización y es el Jefe del departamento de Sistemas.

Los procedimientos generales de petición, autorización, asignación de prioridades, programación y entrega de aplicaciones se describen a continuación:

En cuanto a la petición, los requerimientos por parte de los departamentos se realizan mediante oficio de solicitud de servicio (Anexo 8). Los requerimientos por parte de la dirección general se realizan personalmente en una reunión en la que se definen los objetivos y alcances del sistema. El proyecto es discutido con el área solicitante y dependiendo de la importancia (para el área involucrada) y del costo en tiempo (para Sistemas) se autoriza automáticamente o se plantea en la dirección general. Es decir, algunos proyectos se aceptan directamente por el área de sistemas y otros por el Director General. Las prioridades se definen por la dirección general. Y por último, está la programación y entrega de Aplicaciones, donde toda Aplicación es desarrollada con base en un programa de trabajo en el que se consideran los tiempos de programación por módulo o programa y los tiempos de ejecución de actividades como levantamiento de información, implantación de nuevos procedimientos y capacitación del personal involucrado.

Los criterios que se siguen para el desarrollo de una aplicación son:

- Que sea fácil de operar o amigable.
- Interfaz intuitiva muy similar a las aplicaciones comunes de Windows.
- Se busca la eficacia en los procesos, es decir que se realicen en el menor tiempo posible y funcionen a la perfección
- Especial atención en las búsquedas de información
- Desarrollan la interfaz junto con los usuarios, presentando varias alternativas y seleccionando la mas adecuada.

- Simulan los procedimientos en forma manual, para que el usuario entienda perfectamente como opera el sistema.
- Los informes se generan de tal forma que los usuarios puedan modificarlos, esto agrega versatilidad a la información, ya que se puede utilizar para diferentes propósitos.

Para el desarrollo de aplicaciones sí existe una metodología integrada por el personal del departamento de sistemas, que consiste básicamente en las siguientes etapas:

1. Determinación del problema (Definición de Objetivos).
2. Identificación de procedimientos actuales (Manuales o automatizados).
3. Diseño de nuevos procedimientos y controles (Flujo de datos y validaciones).
4. Revisión y autorización de nuevos procedimientos.
5. Diseño de Estructura de Datos (Base de datos, tablas, relaciones, etc).
6. Diseño de Programa de Trabajo para el área de Sistemas.
7. Diseño de Programa de Trabajo para el área Solicitante.

En la empresa se comprueba que las aplicaciones desarrolladas tuvieron éxito en cada aplicación se puede manejar como objetivos básicos: La obtención de información que permita evaluar la operación y resultados de las áreas involucradas; la optimización de procedimientos; la validación de operaciones criticas o importantes; mantener actualizada la información para facilitar así su procesamiento. De esta forma, en la medida que el sistema logre estos objetivos se determina el grado de éxito que éste alcanza.

Los criterios de calidad que se siguen para las aplicaciones desarrolladas son: El tiempo de desarrollo, funcionalidad (correcto funcionamiento) y logro de los objetivos.

En el caso de las aplicaciones adquiridas o desarrolladas fuera de la organización se comprueba que satisfacen sus necesidades pues se realiza un análisis del software por adquirir en colaboración directa con el proveedor. Se plantean las necesidades y se aclara si el producto las satisface. Además, se consultan empresas que ya cuentan con el software. Y la calidad de estas aplicaciones se comprueba básicamente evaluándose que se cumplan los objetivos del desarrollo o la adquisición considerando rapidez, eficiencia y funcionalidad.

En la empresa se lleva un registro de los reportes de modificaciones y/o correcciones a los sistemas y se plasman en programas de trabajo de mantenimiento de software, así como un reporte de incidencias emitidos por los clientes y usuarios (Anexo 8).

Evaluar la corrección del procedimiento existente para la realización de los cambios de versiones y aplicaciones.

El procedimiento que se sigue para la adquisición de nuevas aplicaciones y cambios de versiones, es primeramente solicitado por el usuario, ya sea software o hardware. Se prosigue con una justificación por escrito de por qué y para qué se solicita, además de la firma. Posteriormente se lleva junto con la orden de compra aceptada por el Administrador de Red al Director General y Gerente General para que sea aprobado y una vez que se autoriza, se adquiere.

La adquisición de nuevas aplicaciones y cambios de versiones se realiza cada vez que se requiere algún equipo; no hay tiempo establecido para dichos cambios.

Para evitar los problemas de integración y las incompatibilidades que pueden plantear los nuevos productos previamente a su implantación, la empresa, antes de instalar cualquier software realiza pruebas en el departamento de sistemas. Una vez realizadas se selecciona la computadora con las características apropiadas para instalarle el software requerido por el departamento solicitante, posteriormente se vuelve a hacer una revisión antes de instalarlo en todas las computadoras que lo requieran.

Una vez instalado el nuevo software o hardware, no existe un plan para la formación de los usuarios finales que vayan a utilizar estos nuevos productos, sin embargo se le da una capacitación al momento de instalarle el producto y además se les entrega un manual del software. En el caso de que la propia empresa desarrolle una aplicación sí se le da una capacitación al empleado. También existe el caso en donde se adquieren aplicaciones gratuitas como las adquiridas en Internet, las cuales son explicadas por los del departamento de Sistemas. Por otro lado no existe un plan de formación para el encargado de mantenimiento cada vez que se adquiere nuevo equipo de cómputo, él mismo estudia los manuales correspondientes.

El procedimiento para la realización de cambios de versiones de los programas desarrollados dentro de la organización se realiza cada vez que se requiere de satisfacer nuevas necesidades, actualmente la empresa se encuentra cambiando todas las versiones desarrolladas anteriormente ya que éstas fueron desarrolladas en condiciones de operación muy distintas a las actuales. El proceso implica un replanteamiento total de los sistemas, es decir, como si se tratara de uno nuevo.

1. Se hace un levantamiento inicial.
2. Se analizan los flujos y procesos actuales.

3. Se definen los objetivos.
4. Se diseñan los nuevos procesos.
5. Se diseña la estructura de datos.
6. Se realiza el diseño detallado (programas, validaciones).
7. Se elabora el programa de trabajo.
8. Se inicia el desarrollo.

Para la actualización de los sistemas operando, se lleva una bitácora por sistema y se auto incrementa la versión cada vez que se actualiza. Todos los programas que son desarrollados por la empresa cuentan con la documentación necesaria. En la siguiente tabla puede observarse la documentación de ellos

.

Tabla 7.1 "Documentación de los Sistemas"

SISTEMA	REQUERIMIENTOS DEL SISTEMA	DIAGRAMAS DE FLUJO	MODELO ENTIDAD RELACION	BASE DE DATOS	DICCIONARIO DE DATOS	MANUAL DE PROCEDIMIENTOS	MANUAL DE USUARIO
FINANCIERO	SI	SI	SI	SI	NO	SI	NO
INVENTARIOS	SI	SI	SI	SI	NO	SI	NO
DESTAJOS	SI	SI	NO	SI	SI	SI	NO
SUBCONTRATOS	SI	SI	NO	SI	SI	SI	NO

Determinar si los usuarios cuentan con suficiente formación y la documentación de apoyo para desarrollar sus tareas de un modo eficiente.

En "La Casita" no existe un plan de formación para garantizar que todo el personal conozca los productos que tiene que utilizar, pero sí se les da a conocer lo que tienen que utilizar y cómo lo van a utilizar, además de tener manuales. Cuando se hace el desarrollo de un nuevo sistema, la empresa convoca a juntas informativas en donde presentan e indican qué hace el nuevo sistema, quiénes lo utilizan y las relaciones entre los departamentos. Al hacer una mejora o actualización de un sistema, el personal recibe formación del cambio surgido.

El departamento de sistemas comprueba el aprovechamiento obtenido por el personal al observar las mejoras en la entrega de reportes, la rapidez en las tareas, la presentación más formal, el interés por conocer nuevos procedimientos, entre otras.

A todo el personal se le entrega documentación básica sobre aplicaciones instaladas, pero aún no reciben documentación de los sistemas desarrollados por la propia empresa.

En caso de ocupar alguna documentación, el personal puede recibirla, sin problema alguno, por el departamento de sistemas.

Una vez adquirida la formación de los productos y la documentación básica, el departamento de sistemas sí comprueba que el personal utilice las posibilidades que ofrece el producto y no simulan procedimientos utilizados en versiones previas o aplicaciones utilizadas con anterioridad.

Y por último, en caso de haber dudas o problemas, el personal tiene que dirigirse al departamento de sistemas para que se los solucionen.

Determinar si el sistema existente se ajusta a las necesidades reales de la organización.

Se comprueba que el sistema existente se ajuste a las necesidades reales de la organización. Actualmente todo el equipo de la empresa se encuentra activo y utilizándose al 100 por ciento. Sin embargo no se tiene un registro de las actividades que ejecuta cada equipo. Y sí existe un registro de las características de cada equipo (Anexo 3,4,5,6 y 7).

Determinar si existen garantías suficientes para proteger los accesos no autorizados a la información reservada de la empresa y la integridad de la misma.

La documentación en materia de seguridad existente en la organización es definida por el mismo perfil de la empresa, más que nada en sistemas de archivos de AutoCad, Bases de Datos, Compras, destajos y finanzas.

Existe control de acceso para los usuarios, cada uno de ellos puede compartir su información con los de su mismo departamento. Además, existen otros usuarios que pueden compartir y obtener información de otros departamentos.

El departamento de sistemas no tiene un registro de incidencias producidas a causa de la seguridad. Para controlar la seguridad utilizan medidas que tienen definidas como son: los respaldos diarios en cintas, cada tres días en disco duro; verificación diaria de la corriente de energía y revisan instalaciones eléctricas.

Las funciones de seguridad de los encargados del departamento de sistemas son: respaldar la información, verificar conexiones y evitar que la información de todos los sistemas y bases de datos no se pierdan o se dañen.

En caso de no respetar las normas de seguridad, no hay sanciones, pero es responsabilidad de los usuarios cumplir con los lineamientos especificados, sin embargo, si continua el incumplimiento por parte de los usuarios, éstos pueden recibir llamadas de atención o en algunos casos un ultimatum.

Los derechos de acceso que se utilizan en la empresa son de sólo lectura y control total. Existen también los derechos de acceso a servidores los cuales pueden ser accesados solamente si ha sido dado de alta por dominios. Estos usuarios a la vez pueden obtener diferentes niveles de acceso (accesos completos y sólo lectura).

Todos los usuarios siguen un mismo procedimiento de identificación para el acceso al sistema, éste es: Nombre de Usuario y Contraseña. Para salir del sistema solamente tienen que desconectarse de la red. No existe una desconexión automática y no tienen horas limitadas.

La persona encargada de autorizar cambios de los derechos de usuarios es el Administrador de la Red y éstos son respetados.

Para controlar el almacenamiento, distribución, modificación de toda la información confidencial solamente el administrador de red puede manejar dicha información almacenándola en disco duro. La distribución de la información confidencial es por correo electrónico en sucursales y aquí es por claves.

Determinar si el procedimiento de generación de las copias de respaldo es fiable y garantiza la recuperación de la información en caso de necesidad

Toda la información que se genera en la empresa siempre está disponible. El procedimiento que siguen para efectuar copias de seguridad es realizar diariamente una copia de respaldo de toda la información, la cual es automática y se realiza a las 8:30 de la noche en cinta; Lunes, Miércoles y Viernes se hace una copia en disco duro en el servidor. Son programadas por el Administrador de la Red así como las copias que se efectúan en disco duro.

Toda esta información que se almacena no tiene un inventario específico, solamente se tiene identificado la copia del respaldo por el día. Sin embargo, esta información sí es debidamente clasificada.

La autorización para accesar a la información confidencial es restringida para los usuarios, solamente los del departamento de sistemas pueden accesarlo.

En “La Casita” no existe información salvaguardada que esté fuera de la empresa, absolutamente toda la información que genera (incluso las de las otras sucursales) está ubicada en Cd. Obregón, y tampoco tienen garantías equivalentes de toda la información que se guarda.

El proceso que se sigue para la recuperación de las copias de seguridad es buscar la información según propiedades como lo son: el día, el nombre del archivo, extensión utilizada. Es muy fácil acceder a las copias de respaldo.

Determinar si está garantizado el funcionamiento ininterrumpido de aquellas aplicaciones cuya caída podría suponer pérdidas de integridad de la información y aplicaciones.

En cuanto a sistemas de alimentación ininterrumpida, sí se cuenta con ellos pero no en toda la empresa. Los sistemas que ellos utilizan para controlar la pérdida de información son los dispositivos No-Break. Éstos no cubren el 100 por ciento de los procesos en los que cuya interrupción podrían ocasionar grandes repercusiones, debido a la falta de No-Break. A la hora en que estos dispositivos entran en función se otorga al servidor 30 minutos extras después del fallo para que puedan finalizar sus procesos y apagar el sistema; y a las demás computadoras otorgan 22 minutos extras.

Determinar el grado de exposición ante la posibilidad de intrusión de virus.

Se cuenta con un programa para evitar la intrusión de virus (Norton Antivirus 5.0). Este programa es actualizado cada mes a través de la Internet. Para evitar que los usuarios introduzcan virus a la red se les informa por correo electrónico cuáles son los nuevos virus para que no abran archivos sin antes vacunarlos.

El proceso que sigue el departamento de sistemas para revisar la posible intrusión de virus es: 1) Detecta el virus, 2) Se investigan las características, y 3) Se le da una solución o vacuna a través del mismo antivirus o Internet.

Determinar si en el entorno ofimático se producen situaciones que pueden provocar infracciones.

No existe una relación de las aplicaciones que precisen de licencias debido a que la mayoría de las aplicaciones carece de ella. Solamente tienen licencias para el sistema operativo Windows 98 y Windows NT, Sistema de control de obras y presupuestos (Opus). Los programas que tienen y que no cuentan con licencias son: Visual Basic 6.0, AutoCad 14, SQL Server 7.0, Office 97, Corel Draw 9.0, Sygate 2.0, Internet Explorer 4.0 y 5.0, Windows 2000, Crystal Report y Wingate.

8. Fecha del Informe

La fecha del informe es del 18 de octubre de 2000 y las actividades realizadas abarcaron del 21 de Agosto al 13 de Octubre del presente año.

9. Identificación y firmas de los auditores

Los auditores de esta Auditoría de la Ofimática son: Elianna Villa Valdez y Nidia Mondragón Orozco.

10. Distribución del Informe

Las personas que pueden hacer uso del informe son el Director General, Gerente General, el Administrador de la Red y el Jefe de Sistemas de la empresa “La Casita”.

4.2 Discusiones.

Posteriormente se analizaron los resultados reluciendo todo lo referente a cada objetivo para su discusión correspondiente y se observó:

En cuanto al punto de determinar si el inventario ofimático refleja con exactitud los equipos de aplicaciones existentes en la organización, se observó que al tener definidos mecanismos para garantizar que todos los equipos adquiridos en la organización son debidamente inventariados, esto ayuda a la organización debido a que un inventario poco fiable puede repercutir en el

balance de la misma, posibilitando que no se detecten sustracciones de equipamiento informático o de licencias de programas contratadas, haciendo mención de esto Piattini y Del Peso, (1998).

En el punto de determinar y evaluar el procedimiento de adquisiciones de equipos y aplicaciones se encontró que:

- La empresa cuenta con una política de adquisiciones centralizada en la que en el departamento de sistemas es el encargado de realizar las compras de equipo y aplicaciones.

Al contar con una política de adquisiciones centralizada la empresa podría aprovechar los beneficios que ésta puede traer. Piattini y Del Peso, (1998) afirman, que en caso de que los diversos departamentos de la compañía realicen pedidos sobre equipos y complementos de una manera independiente se estará desaprovechando la posibilidad de negociar descuentos mediante la aplicación de una política centralizada de compras.

- Se comprobó que se valoran aspectos relativos a la necesidad real de los equipos solicitados, evaluando si lo que solicitan es realmente necesario, preguntándole al departamento solicitante: ¿Qué ocupan?¿ Para qué lo ocupan? ¿Cuánto lo ocupan?

Con esto se comprueba que en el procedimiento de adquisición se valoran aspectos relativos con el sistema existente, según Piattini y Del Peso, (1998). Ayudando a la empresa a no invertir erróneamente sus recursos financieros, en equipos y aplicaciones innecesarias.

En el objetivo de determinar y evaluar la política de mantenimiento definido en la organización se encontró:

- En la empresa “La Casita” no cuenta con contratos de mantenimiento, pero si utilizan las garantías de los productos adquiridos en cuestión de disco duro y tarjetas de red. También se conoce el estado de las garantías de cada uno de los productos, las cuales casi siempre son de un año y conocen el mecanismo para hacerla efectiva y el que ellos utilizan son la copia de la factura y el equipo.

Con esto se observa que en la empresa, los usuarios finales conocen el estado de las garantías de cada uno de los productos que utilizan y los mecanismos para hacerlas efectivas, afirman Piattini y Del Peso, (1998). Logrando con esto un ahorro en la inversión requerida al no tener que desperdiciar esas garantías al hacerlas efectivas.

- En el momento en que la garantía caduca la empresa ya se hace responsable del producto. También se conocen los productos en los que la responsabilidad del mantenimiento recae en la propia empresa.

Piattini y Del Peso, (1998) recomiendan, que se determinen cuáles productos disponen de contratos de mantenimiento vigentes con empresas externas y cuáles son aquellos en los que la responsabilidad del mantenimiento recae en la propia organización.

- El que no existan contrataciones de mantenimiento con empresas externas no llega a repercutir en la organización ya que sí se encuentra una persona capacitada y asignada para realizar las tareas de mantenimiento, siendo éste el Administrador de la Red.

Piattini y Del Peso, (1998), afirman que se debe comprobar que el personal, tanto interno como externo, asignado en tareas de mantenimiento tiene suficientes conocimientos de las plataformas que debe mantener, y que recibe la información adecuada sobre los nuevos productos instalados en la organización.

En el punto de evaluar la calidad de las aplicaciones del entorno ofimático desarrollado por personal de la propia organización, se encontró:

- En la empresa "La Casita" existe un responsable de controlar el desarrollo de aplicaciones de toda la organización y es el Jefe del departamento de Sistemas. Se tienen definidos procedimientos generales de petición, autorización, asignación de prioridades, programación y entrega de aplicaciones. Los demás departamentos no desarrollan sus propias aplicaciones sino el departamento de sistemas es el departamento responsable de realizarlos con sus propios criterios de desarrollo de aplicación y que están de acuerdo con el usuario.

Según Piattini y Del Peso (1998), el equipo auditor determinará la existencia de un departamento responsable de controlar el desarrollo de aplicaciones de toda la organización, y que se han definido procedimientos generales de petición, autorización, asignación de prioridades, programación y entrega de aplicaciones, o bien si los departamentos han desarrollado aplicaciones de uso interno, bajo sus propios criterios, sin control de un departamento responsable.

- En la empresa se lleva un registro de los reportes de modificaciones y/o correcciones a los sistemas y se plasman en programas de trabajo de mantenimiento de software, así como un reporte de incidencias emitidos por los clientes y usuarios. (Anexo 8)

Es tarea del equipo auditor examinar el reporte de incidencias de las aplicaciones, así como las reclamaciones manifestadas por los clientes y usuarios como indicios para detectar aquellas aplicaciones que podrían estar funcionando de un modo anómalo; afirman Piattini y Del Peso, (1998).

Otro de los objetivos fue evaluar la corrección del procedimiento existente para la realización de los cambios de versiones y aplicaciones, donde se encontró que:

- En la empresa se sigue un procedimiento para la adquisición de nuevas aplicaciones y cambios de versiones, también en los que son desarrollados por la propia empresa. Por lo tanto, se comprueba lo que Piattini y Del Peso, (1998) que recomiendan determinar la existencia de procedimientos formalmente establecidos para la autorización, aprobación, adquisición de nuevas aplicaciones y cambios de versiones.
- Cuando se requiere de realizar implantaciones, para evitar problemas de adaptación de los sistemas viejos con los nuevos, la empresa realiza pruebas en diferentes computadoras. Una vez aceptado el nuevo sistema se les da una capacitación a los usuarios finales.

Con esto se ha revisado lo que Piattini y Del Peso, (1998) señalan que también el equipo auditor se ocupará de determinar si se han analizado los problemas de integración y las incompatibilidades que pueden plantear los nuevos productos previamente a su implantación; si se ha establecido algún plan para la formación de los usuarios finales que vayan a utilizar estos nuevos productos.

En cuanto al punto de determinar si los usuarios cuentan con suficiente formación y la documentación de apoyo para desarrollar sus tareas de un modo eficaz y eficiente.

- El que no exista un programa en donde el personal de la empresa reciba una capacitación sobre los productos que tenga que utilizar, esto no llega a afectar a la empresa para realizar sus tareas. El personal tiene el compromiso de adquirir conocimientos por medio de los manuales que pueden obtener en la misma organización.

Con esto se comprueba que en la empresa si se tiene una formación para garantizar que todo el personal conoce los productos que se tienen que utilizar, incluyendo las nuevas aplicaciones y las versiones instaladas, esto es según Piattini y Del Peso, (1998).

- Ya que se realiza la formación a los usuarios finales puede comprobarse que hubo aprovechamiento por parte de ellos, debido a que pueden observarse cambios en los trabajos que realicen posteriormente. Los empleados obtienen rápidamente documentación y ayuda en caso de requerirla.

Según Piattini y Del Peso, (1998) se debe comprobar el aprovechamiento conseguido, y si se entrega la documentación básica de la operativa del producto, o si se pueden acceder a ella fácilmente en caso de necesidad.

En el objetivo de determinar si existen garantías suficientes para proteger los accesos no autorizados a la información reservada de la empresa y la integridad de la misma.

- ♣ Toda la información que se genera puede ser accesada por todos los usuarios, pero se asignan ciertos privilegios según el puesto que desempeñen. En ocasiones pueden surgir problemas de seguridad física, incidencias que los del Departamento de Sistemas no registran. Las medidas que ellos utilizan son: respaldos de información y verificación de las conexiones. Para la seguridad lógica, se crean restricciones de acceso según el usuario y si en algún momento se observan malos manejos en cuanto a sus contraseñas, pueden ser notificados por la gerencia.

Según Piattini y Del Peso, (1998), el equipo auditor examinará la documentación en materia de seguridad existente en la organización y comprobará que han sido definidos, al menos, procedimientos de clasificación de la información, control de acceso, identificación y autenticación, gestión de incidencias y controles de Auditoría. Con posterioridad pasará a comprobar si las medidas de seguridad definidas se encuentran realmente operativas.

Al determinar si el procedimiento de generación de las copias de respaldo es fiable y garantiza la recuperación de la información en caso de necesidad se observó:

- La seguridad de la información en la empresa es muy importante, para lograr esto se efectúan copias diariamente; algunas realizadas por el mismo Administrador de la Red y otras son programadas automáticamente.

Según Piattini y Del Peso, (1998), la información generada por el sistema debe estar disponible en todo momento. La no disponibilidad de datos, especialmente de aquellos procedimientos críticos para la organización, además de las consabidas pérdidas económicas, podría llevar, en el extremo, a la paralización del departamento. El equipo auditor examinará el procedimiento de copias de seguridad seguido en la organización, verificando la suficiencia de la periodicidad, la correcta asignación de responsabilidades y el adecuado almacenamiento de los soportes.

- ♣ Toda esta información que se almacena no tiene un inventario específico, solamente se tiene identificado la copia del respaldo por el día. Sin embargo esta información sí es debidamente clasificada.

Para Piattini y Del Peso, (1998), se verificará la existencia de un inventario de los soportes que contienen las copias de seguridad y de la información salvaguardada.

- El acceso a la información confidencial es restringida para los usuarios, solamente los del departamento de sistemas pueden accesarlo. No existe información salvaguardada que esté fuera de la empresa, absolutamente toda la información que genera está ubicada en Cd. Obregón, y tampoco manejan garantías de la información que se guarda.

Piattini y Del Peso ,(1998), indican que posteriormente, se determinará si la seguridad implementada para garantizar la confidencialidad e integridad de las copias de salvaguarda ofrece garantías equivalentes a las definidas para la información que contienen, tanto en los soportes que se mantienen en los locales de la empresa como en aquellos que se trasladan en una ubicación externa.

El siguiente punto es el de determinar si está garantizado el funcionamiento ininterrumpido de aquellas aplicaciones cuya caída podría suponer pérdidas de integridad de la información y aplicaciones.

- En cuanto a sistemas de alimentación ininterrumpida, manejan los dispositivos No-Break. Éstos llegan a controlar la pérdida de información en un alto porcentaje, pero la empresa cuentan con pocos dispositivos.

En las organizaciones se desarrollan procesos en los que una caída de tensión podría ocasionar pérdidas de integridad de la información y aplicaciones manejadas, en ocasiones irrecuperables, afirman Piattini y Del Peso, (1998).

El equipo auditor determinará la existencia de sistemas de alimentación ininterrumpida, y si éstos cubren el funcionamiento de aquellos equipos en los que se ejecutan procesos cuya interrupción podría ocasionar graves repercusiones, según Piattini y Del Peso, (1998).

Al determinar el grado de exposición ante la posibilidad de intrusión de virus se encontró:

- Se cuenta con un programa para evitar la intrusión de virus (Norton Antivirus 5.0). Este programa es actualizado cada mes a través de la Internet. Para evitar que los usuarios introduzcan virus a la red se les informa por correo electrónico cuáles son los nuevos virus para que no abran archivos sin antes vacunarlos.

Para Piattini y Del Peso, (1998), los costos derivados de la intrusión de virus informáticos se han multiplicado en los últimos años: pérdida de la información y empleo de recursos y tiempo

para restablecer el sistema, llegando en algunos casos a la paralización temporal del departamento.

En cuanto al objetivo de determinar si en el entorno ofimático se producen situaciones que pueden provocar infracciones se observa:

- No existe una relación de las aplicaciones que precisen de licencias debido a que la mayoría de las aplicaciones carece de ella.

Para Beekman, (1995) al comprar un paquete corriente de software, en realidad no está comprando el software, sino una licencia de software que le permite usar el programa en la máquina. Los acuerdos de licencia varían de una compañía a otra, pero la mayoría incluye limitaciones en cuanto al derecho del usuario a copiar discos, instalar software en discos duros y transferir información a otros usuarios. Casi todos los productos de software comercial en el mercado tienen derechos de autor, de modo que no pueden duplicarse legalmente para ser distribuidos a terceros; algunos discos están protegidos contra copias, de manera física, para que no puedan copiarse. La creación de software es increíblemente costosa, debido a su dificultad. La mayoría de los creadores de software usan los derechos de autor y la protección contra copias para asegurarse de que vendan suficientes copias de sus productos para recuperar su inversión seguir operando y escribir más programas.

Con esto se concluye que al aplicarse la Auditoría de la Ofimática se conoció que el aprovechamiento de los recursos ofimáticos en esta empresa son los adecuados.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

La aplicación de una buena Auditoría Ofimática puede traer como consecuencia resultados positivos, ya que sin duda alguna se pretende que mediante su aplicación, una empresa pueda reconocer y aceptar que aprovecha o no los recursos con los cuales actualmente está trabajando, y conocer realmente si su información es manejada adecuadamente y con la suficiente seguridad que se necesita para mantener la integridad de los datos.

Al realizar la auditoría, basándose principalmente en las entrevistas y cuestionarios permite a los auditores detectar la existencia de problemas o deficiencias, dando la posibilidad a los auditores de ocuparse de las deficiencias en el funcionamiento de la organización, pero además contribuir en conocimientos para la elaboración de mejores alternativas y recomendaciones. En este capítulo se mostrarán las conclusiones y recomendaciones al realizar una Auditoría Ofimática en la empresa “La Casita”.

5.1 Conclusiones.

Se cumple el objetivo de proporcionar herramientas necesarias para que la organización pudiera cubrir todas sus necesidades de la oficina y tener una mejor distribución de información.

En cuanto a Economía, Eficiencia y Eficacia lo primero que se tiene que hacer es comprobar que se realiza un inventario de todo el equipo y aplicaciones que son adquiridas en la empresa, ya que es importante porque sino la empresa no puede tener un inventario fiable y esto pueda repercutir en el balance de la organización, posibilitando que no se detecten sustracciones de equipamiento informático o de licencias de aplicaciones.

La manera en que las empresas realizan la compra de equipo y aplicaciones puede repercutir sobre todo en significativas pérdidas de dinero, porque puede que realmente el equipo que se está solicitando no sea urgente o quizás otro equipo que se tenga pueda satisfacer las necesidades de lo que algún departamento esté requiriendo. Más que nada hay que comprobar que realmente se requiere y que si la falta de él ocasionaría un mal funcionamiento.

Cuando una empresa requiere de tanto equipo y aplicación, la necesidad de tener un control de mantenimiento de sus equipos es indispensable porque ocasiona que no se tenga conocimiento de las garantías de los productos y la expiración de ellas.

Un Sistema Informático desarrollado y mal diseñado, tanto interna como externamente, puede convertirse en una herramienta peligrosa para la empresa: como las máquinas obedecen las órdenes recibidas y el funcionamiento de la empresa está determinada por las computadoras que materializan los Sistemas de Información, la gestión y la organización de la empresa no puede depender de un Software y Hardware mal diseñados.

En el momento en que se soliciten cambios de aplicaciones o de versiones, primeramente debe analizarse si realmente solucionan los problemas que han venido a través del tiempo, y también verificar si no los ocasiona en cuanto a compatibilidad con la aplicación ya instalada.

No queda por demás ofrecer a los usuarios de los sistemas una buena capacitación de los equipos y las aplicaciones que se utilizan dentro de la empresa, así como de las nuevas aplicaciones que se vayan a desarrollar. Ya que sin duda alguna, el usuario es el elemento más importante dentro de una empresa y al contar con suficientes conocimientos ofrecidos por parte de la empresa, estarán motivados para trabajar de un modo más eficiente y eficaz.

El hecho también de analizar el equipo y aplicaciones que se encuentren obsoletos dentro de una empresa, puede proporcionar suficientes mejoras en cuanto a la utilización de los sistemas, y lograr una mejor distribución y utilización de las mismas aplicaciones, evitando así pérdidas de tiempo y futuros problemas.

En cuanto a Seguridad, las computadoras son un instrumento que estructuran gran cantidad de información que es muy importante para los individuos y la empresa, y puede ser peligrosa para la organización si es mal utilizada o divulgada a personas que hagan mal uso de ésta. También pueden ocurrir 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 costosos. Es de vital importancia tener un control de accesos a personas ajenas a la empresa, y por supuesto mantener un control y elaborar niveles de acceso a la información.

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar: el llamado "virus informático", el cual, aunque tiene diferentes intenciones, se encuentra principalmente para paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco. Al haber auditado los sistemas no deben tener copias "piratas" o bien que, al conectarse 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.

Existen métodos eficaces para proteger sistemas de información como son los software de controles 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. Dichos paquetes han sido populares desde hace muchos años en el mundo de las computadoras grandes, y los principales proveedores ponen a disposición de sus clientes algunos de estos paquetes.

Además de tener el control de accesos, es importante realizar los respaldos de toda la información que se genera dentro de la empresa así como tenerlos para cuando se requiera alguna información en específico. Al realizar los respaldos se pueden evitar pérdidas de información en caso de que ocurriera algún accidente, pero también sirve para tener mejor clasificada la información y llevar un control de la información. Y por consecuencia de la clasificación debe tenerse siempre a la mano y de fácil acceso.

La seguridad es también contar con sistemas de alimentación ininterrumpida para evitar pérdidas de información al instante, ya que un apagón podría resultar catastrófico para la empresa

si en ese momento están concluyendo con un proceso importante y se pierda toda la información sin guardar. Mediante el uso de estos sistemas ayudan a proteger la información permitiendo así guardar y salir del sistema.

Concluyendo con el estudio, se puede verificar con facilidad, como la empresa tiene bien asignados todos los recursos con los que cuenta y éstos son utilizados de manera eficaz.

Al realizar el estudio se necesitaba del departamento de sistemas. Se contó con suficiente participación por parte de los encargados del departamento, obteniendo toda la información que se necesitaba, además se dio la posibilidad de verificarla, valiéndose de los formatos que fueron proporcionados para su correspondiente comprobación. También se revisaron los sistemas de información con los que actualmente cuentan y con los que están en desarrollo. Por otro lado, se permitió realizar una revisión al equipo de cómputo y sus aplicaciones correspondientes.

Una vez realizada la auditoría, se hizo una recopilación de datos y se analizó para proporcionar en su momento el informe de auditoría ofimática. El informe está realizado de una manera entendible y sencillo para que la empresa no tenga problema alguna al momento de leerla.

La aplicación de la auditoría ofimática sirve bastante a la empresa, sobre todo si se encuentran síntomas de desorganización y descoordinación, mala imagen e insatisfacción de los usuarios, síntomas de inseguridad y elevados costos. Como consecuencia de lo anterior, se aplica la auditoría y se proporcionan ciertos puntos que la empresa no tenía considerados como buenos y de gran utilidad, puntos que serán dados a conocer en las recomendaciones.

Por otro lado, en este estudio se obtiene un conocimiento enorme en lo que implica el aprovechar todos los recursos de una manera eficiente y eficaz de una empresa; y sobre todo la seguridad que se debe contar, ya que si ocurriera alguna pérdida de la información, sería casi la destrucción de la organización.

5.2 Recomendaciones

Hoy en día, los entornos ofimáticos han constituido herramientas poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial como lo son los Sistemas de Información de la empresa y los equipos computacionales.

"La Casita" es una empresa que actualmente cuenta con lo suficiente para estar dando lo mejor de sí, trabajan con organización y siempre están en constante cambio, y así debe ser, porque la tecnología avanza demasiado rápido y si no se va acorde a ella se está realizando un trabajo mediocre y sin la rapidez con la que se tendría al contar con determinada tecnología que ayuda a agilizar los procesos, ahorrar tiempo y dinero.

La finalidad de la aplicación de la auditoría ofimática no es realizar una simple revisión de sus equipos y aplicaciones, ni tampoco es reclamar en lo que anda mal, sino todo lo contrario: ofrecer mejores soluciones para la reducción de pérdidas de tiempo en malos manejos de información y de los propios equipos.

En lo que se refiere a Economía, Eficacia y Eficiencia, se recomienda que se elaboren políticas más definidas de mantenimiento como sería elaborar programas que ayuden al encargado de realizar el mantenimiento, especificando la fecha en la que se realizará el mantenimiento y a qué máquinas se le dará para que estén disponibles y se pueda trabajar lo más rápido posible en ellas para no interrumpir en el funcionamiento de la organización. También que se establezca un formato en donde se registren las incidencias producidas, para llevar así un mejor control de los problemas que se han ocasionado, qué los ha ocasionado, cuándo se ocasionaron, cómo se solucionaron, quién lo realizó, etc.

En cuanto al uso de los sistemas por parte de los usuarios, es recomendable ofrecer cursos de los sistemas de información para que el usuario tenga una noción completa de ellos además de incrementar sus conocimientos.

Es muy importante tener un registro de todas las actividades que se realizan en cada equipo de cómputo evitando así tener duplicaciones de información o de aplicaciones, evitándose también que existan datos o aplicaciones extras que pueden alentar al equipo de cómputo.

Y para cuando se desarrollen sistemas de información dentro de la empresa, es recomendable realizar aparte de la documentación que actualmente elaboran, los manuales de los usuarios, para así en caso de que los usuarios tengan una duda en el sistema pueden consultarlo.

En lo que se refiere a la seguridad, se recomienda que existan sanciones en caso de incumplimiento a las normas de seguridad para que así el empleado tenga más conciencia de la importancia de la información. También realizar un registro de incidencias producidas. Con información que proporcione: día, causa, solución, encargado, si se compró equipo, etc. Generar un inventario de copias de seguridad también es recomendable para la empresa, en donde se controle: archivos que se guardaron, fecha, espacio ocupado, hora, etc. logrando con esto que al momento de requerir información se obtenga sin ningún problema y rápidamente. Además de que la información que se guarde en cintas, pudiera tener etiquetas que las identifique.

Se recomienda a la empresa que tenga información salvaguardada externamente, ya que si ocurriera algún incidente, perdería totalmente toda la información. Lo que se recomendaría es que tuviera un respaldo por medio del servidor en cualquiera de las sucursales. Asimismo para evitar pérdidas en un apagón es recomendable la compra de más dispositivos No-Break.

Asimismo, se sugiere que se analice la posibilidad de adquirir las licencias de las aplicaciones que carecen de ella, ya que si son descubiertas las aplicaciones que carecen de licencia podría ocasionar a la organización multas muy costosas.

En general, se recomienda a la empresa realizar la Auditoría Ofimática cada seis meses para detectar las anomalías que han surgido y corregirlas a tiempo.

La organización podría solicitar una Auditoría Ofimática a una persona capacitada para realizarla como lo es un Licenciado en Sistemas de Información Administrativa; también podría poner su propio departamento de Auditoría de Sistemas; o bien, si la empresa considera que le resultaría algo costoso el contratar a un profesional en el área o destinar un departamento que sea especial para realizarla, puede asignársele a una persona de su misma organización que conozca todo lo referente a los Sistemas de información, equipos de cómputo y aplicaciones que se utilizan, cómo son sus adquisiciones, el manejo de su inventario, el conocer si los usuarios del departamento que solicitan equipo o aplicaciones éstas son las que realmente necesitan, entre otras cosas que son de gran importancia para la realización de esta trabajo.

En caso de que esta empresa opte por asignarle este trabajo extra a una o varias personas de su misma organización, en este caso se le recomienda que las personas que realicen la

Auditoría ofimática sea el administrador de la red y el jefe del departamento de sistemas; ya que el administrador de la red conoce todo lo referente al equipo de cómputo y aplicaciones, así como el manejo del inventario y de las adquisiciones de sistemas; éste a su vez lo puede auxiliar el jefe del departamento de sistemas para completar la Auditoría de la ofimática, ya que él puede contribuir con la información referente a los sistemas de información que se desarrollan dentro de la organización y pueden idear mejoras para la impartición de los cursos de los sistemas de información a los usuarios, entre otras cosas que se vayan dando en su realización.

Sin embargo, la ventaja de contratar a un profesional en el área como lo sería un Licenciado en Sistemas de Información Administrativa, es que es una persona externa a la organización y su resultado estará dado a lo que realmente se obtuvo en su investigación, sin la preocupación de que lo que diga en su informe podría perjudicar en su trabajo al detectarse irregularidades en caso de que el auditor sea el personal de la misma organización; otra de las ventajas es que un Licenciado en Sistemas de Información Administrativa es una persona que tiene mayores conocimientos en el área y puede dar una información más específica en el resultado que se obtenga y los puntos a revisarse.

Cabe mencionar que si la empresa cuenta con suficientes recursos económicos, se le recomienda la posibilidad de tener su propio departamento de Auditoría de Sistemas de Información (Auditoría Informática), donde no sólo realizarían la Auditoría Ofimática regularmente, sino que también auditaría todo lo referente a las Bases de Datos, Redes, Seguridad Física, Seguridad Lógica, Control Interno, entre otras que se realizan en una auditoria de Sistemas de Información, donde una Auditoría informática sustenta y confirma la consecución de los Objetivos de protección de activos e integridad de los datos y Objetivos de gestión que abarcan, no solamente los de protección de activos, sino también los de eficacia y eficiencia; asimismo, tiene la finalidad de evaluar y controlar total o parcialmente un sistema informático, con el fin de proteger sus actividades y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general en cada empresa, y para conseguir la eficacia exigida en el marco de la organización correspondiente.

La decisión será dependiendo de la empresa y ésta verá cual es la opción que mejor se adapte a sus necesidades y que cumpla mejor sus objetivos.

REFERENCIAS BIBLIOGRÁFICAS

Beekman George, “Computación e Informática Hoy”, 1ra. Edición, Editorial Adisson Wesley, México, 1995.

Cohen Daniel, “Sistemas de Información para la toma de decisiones”, 2ª Edición, Mc Graw Hill, México, 1996.

Levin Richard B., “Virus Informático”, 1ra. Edición, Editorial Mc Graw Hill, México, 1992.

Mueller Scott, “Manual de Actualización y Reparación de PC´s” 11va. Edición, Editorial QUE, México, 1999.

Piattini Mario y Del Peso Emilio, “Auditoría Informática. Un enfoque práctico.”, 1ra. Edición, Editorial AlfaOmega, México, 1998.

Seen James A., “Análisis y Diseño de Sistemas de Información”, 1ra. Edición, Editorial Mc Graw Hill, México, 1992.

1999, “Auditoría Informática”, canavia@infovia.com.ar, http://www.essaynetwork.com/trabajos/auditoinfo/auditoinfo.html

APÉNDICE A

La entrevista que se efectuó en la empresa fue la siguiente:

1. ¿A qué se dedica esta empresa?
2. ¿Cuentan con sucursales?
3. ¿Cuentan con departamento de Sistemas?
4. ¿Dónde tienen concentrada la información?
5. ¿Quién maneja la información?
6. ¿Quiénes son las personas encargadas del manejo equipo de cómputo y aplicaciones?
7. ¿Cuáles son los puestos que desempeñan?
8. ¿Cuál es la descripción de los puestos?
9. ¿Qué persona podría autorizar una Auditoría Ofimática?

APÉNDICE B

El cuestionario utilizado para la realización de la Auditoría Ofimática es el siguiente:

ECONOMIA, EFICACIA Y EFICIENCIA

Determinar si el inventario ofimático refleja con exactitud los equipos de aplicaciones existentes en la organización.

1. ¿Se tienen registros de todas las compras de componentes que realiza la organización?
2. ¿Cómo se tienen registradas las compras?
3. ¿Qué procedimiento se utiliza para la autorización de compra dentro de la organización?
4. ¿Se realiza inventario de todo el equipo adquirido?
5. ¿Cada qué tanto tiempo se realiza este inventario?
6. ¿Cuándo se actualiza este inventario?
7. ¿Existe alguna persona encargada de controlar este inventario?

Determinar y evaluar el procedimiento de adquisiciones de equipos y aplicaciones.

8. ¿Se cuenta con una política de adquisición de equipo y aplicaciones?
9. ¿Se valoran aspectos relativos a la necesidad real de los equipos solicitados y a la integración de dichos equipos con el sistema existente? ¿Cómo?
10. En el caso de compra de paquetes o de contratación de externos ¿Se determina si las prestaciones ofrecidas por el producto solicitado se ajustan a las actividades que se pretenden desarrollar con él? ¿Cómo?
11. Al realizar lo anterior ¿Se prevee que las plataformas en las que van a estar instaladas las aplicaciones tengan suficiente capacidad para soportarlas de un modo eficiente? ¿Cómo se lleva a cabo?
12. ¿Cuál es el procedimiento que se sigue para realizar compras de equipo y aplicaciones dentro de la organización?

13. ¿Se realiza compra de equipo y aplicaciones de manera independiente por cada departamento?

Determinar y evaluar la política de mantenimiento definido en la organización.

14. ¿Cuenta la organización con políticas de mantenimiento? ¿Cuáles son?
15. ¿Cuenta con contratos de mantenimiento?
16. ¿Utilizan las garantías de los productos adquiridos?
17. ¿Se conoce el estado de las garantías de cada uno de los productos que utilizan y los mecanismos para hacerlas efectivas?
18. En caso de que la garantía de los productos haya caducado. ¿Se conoce cuáles disponen de contratos de mantenimientos vigentes con empresas externas?
19. ¿Se conoce cuáles son aquellos productos en los que la responsabilidad del mantenimiento recae en la propia organización?
20. A la hora de realizar contrataciones con empresas externas ¿Se verifica si se incluye en el contrato aspectos como el tiempo máximo de respuesta, recambios y mano de obra, mantenimiento preventivo, etc.? ¿Cuáles son los aspectos que se manejan en la empresa?
21. ¿Existe personal de mantenimiento?
22. ¿Reciben capacitación sobre los nuevos productos instalados?
23. Respecto a las incidencias producidas ¿Se tiene un registro de las incidencias producidas?
24. ¿Existen procedimientos establecidos para asignar recursos para solucionarlas? ¿Cuáles son?
25. ¿El tiempo utilizado para atender las solicitudes y las incidencias producidas pueden llegar a afectar el buen funcionamiento de la organización?. En caso de que la respuesta sea negativa ¿Qué es lo que hacen para que las incidencias no afecten al buen funcionamiento de la organización?

Evaluar la calidad de las aplicaciones del entorno ofimático desarrollado por personal de la propia organización.

26. ¿Existe una persona responsable de controlar el desarrollo de aplicaciones de toda la organización?
27. ¿Cómo son manejados los procedimientos generales de petición, autorización, asignación de prioridades, programación y entrega de aplicaciones?
28. ¿Qué criterios se siguen para el desarrollo de una aplicación?
29. ¿Existe una metodología para el desarrollo de aplicaciones? ¿Cuál es?
30. ¿Cómo comprueban que la aplicación desarrollada tuvo éxito?
31. ¿Cuáles son los criterios de calidad para las aplicaciones desarrolladas?
32. En el caso de las aplicaciones adquiridas o desarrolladas fuera de la organización. ¿Cómo comprueban que pueden satisfacer sus necesidades?
33. ¿Cómo comprueban la calidad de estas aplicaciones?
34. ¿Existe un reporte de incidencias de las aplicaciones?
35. ¿Existe un reporte de incidencias emitidos por los clientes y usuarios?

Evaluar la corrección del procedimiento existente para la realización de los cambios de versiones y aplicaciones.

36. ¿Cuáles son los procedimientos establecidos para la autorización, aprobación, adquisición de nuevas adquisiciones y cambios de versiones?
37. ¿Cada cuánto tiempo se realiza lo anterior?
38. ¿Quién los autoriza?
39. ¿Cuál es el procedimiento que se sigue para los cambios de versiones?
40. ¿Cómo se analizan los problemas de integración y las incompatibilidades que pueden plantear los nuevos productos previamente a su implantación?
41. ¿Programan algún plan para la formación de los usuarios finales que vayan a utilizar estos nuevos productos?
42. ¿Programan un plan para los encargados de mantenimiento?

43. ¿Cuál es el procedimiento que se sigue para los cambios de versiones de los programas desarrollados dentro de la organización?
44. ¿Se cuenta con la documentación de cada uno de los sistemas que se han desarrollado dentro de la empresa? ¿Cuáles sí y cuáles no?
45. ¿Se tienen documentados los requerimientos del sistema?
46. ¿Se tienen documentados los Diagramas de Flujo?
47. ¿Se tiene documentado el Modelo Entidad Relación o Relacional?
48. ¿Se documenta la Base de Datos?
49. ¿Se realiza un diccionario de datos para documentar el Diseño del Sistema?
50. ¿Se realiza el Manual de operación de cada Sistema?
51. ¿Se realiza el Manual de Usuario de cada Sistema?

Determinar si los usuarios cuentan con suficiente formación y la documentación de apoyo para desarrollar sus tareas de un modo eficaz y eficiente.

52. ¿Existe un plan de formación para garantizar que todo el personal conoce los productos que tiene que utilizar?
53. ¿Cada qué tanto tiempo se les da al personal formación de los productos?
54. ¿Cómo comprueban el aprovechamiento obtenido por el personal?
55. ¿Se entrega documentación básica de la operativa del producto?
56. En caso de que no se entregue la documentación básica de la operativa del producto. ¿Se puede acceder a ella fácilmente en caso de necesidad?
57. ¿Cuál es el procedimiento que se sigue para poder accesar a la documentación básica de la operativa del producto?
58. ¿Se comprueba que el personal utiliza las posibilidades que ofrece el producto y no simulan procedimientos utilizados en versiones previas o en aplicaciones utilizadas con anterioridad?
59. En caso de haber dudas o problemas en cuanto al producto. ¿Cómo se soluciona el problema?: 1) Mediante un equipo de soporte común en toda la organización. 2) El propio departamento.

Determinar si el sistema existente se ajusta a las necesidades reales de la organización.

60. ¿Existe una relación del equipo que no se encuentra operando?
61. ¿Tienen registradas las actividades que se ejecutan en cada equipo?
62. ¿Tienen registradas las características de cada equipo?

SEGURIDAD

Determinar si existen garantías suficientes para proteger los accesos no autorizados a la información reservada de la empresa y la integridad de la misma.

63. ¿Existen procedimientos de seguridad en la empresa?
64. ¿Tienen clasificada toda la información que se maneja? ¿Cómo?
65. ¿Tienen control de acceso para los usuarios? ¿Cómo los clasifican?
66. ¿Tienen controlado el registro de incidencias producidas a causa de la seguridad?
67. ¿Qué medidas de seguridad tienen definidas?
68. ¿Qué funciones, obligaciones y responsabilidades de seguridad tienen los encargados de los sistemas de información?
69. ¿Qué funciones, obligaciones y responsabilidades de seguridad tienen todos los usuarios de los sistemas?
70. ¿Existen sanciones en caso de no hacer caso a la seguridad?
71. ¿Qué tipos de derechos de acceso utilizan en la empresa?
72. ¿Existen procedimientos de identificación y autenticación para el acceso al sistema?
73. ¿Cómo controlan el almacenamiento, distribución, modificación de toda la información confidencial?
74. ¿Existe una desconexión automática para los usuarios? ¿Tienen horas limitadas? ¿Cada quién se desconecta? ¿Por período inactivo?
75. ¿Quiénes son las personas encargadas de autorizar cambios en los derechos de usuarios? ¿Son respetados?

Determinar si el procedimiento de generación de las copias de respaldo es fiable y garantiza la recuperación de la información en caso de necesidad.

76. ¿La información generada por el sistema está disponible en todo momento?
77. ¿Existen procedimientos de copias de seguridad? ¿Cómo las hacen? ¿En dónde se almacena la información?
78. ¿Cada cuánto tiempo se realizan las copias de seguridad?
79. ¿Quién realiza las copias de seguridad?
80. ¿Existe un inventario de copias de seguridad?
81. ¿Está la información debidamente clasificada?
82. ¿Puede disponerse de ella rápidamente?
83. ¿Quién autoriza el acceso a la información confidencial?
84. ¿Existe información salvaguardada que esté fuera de la empresa?
85. ¿Tienen garantías equivalentes de toda la información que se guarda?
86. ¿Cómo es el proceso para la recuperación de las copias de seguridad?

Determinar si está garantizado el funcionamiento ininterrumpido de aquellas aplicaciones cuya caída podría suponer pérdidas de integridad de la información y aplicaciones.

87. ¿Existen sistemas de alimentación ininterrumpidas?
88. En caso de que se tengan. ¿Cubren todo el funcionamiento de aquellos equipos en los que se ejecutan procesos cuya interrupción podría ocasionar graves repercusiones?
89. ¿Cuánto tiempo de actividad es proporcionado a la hora de que entran estos sistemas?
90. ¿Alcanzan a terminarse los procesos críticos y apagar el sistema?

Determinar el grado de exposición ante la posibilidad de intrusión de virus.

91. ¿Tienes programas encargados de evitar la intrusión de virus?
92. ¿Cuál programa utilizan?
93. ¿Cada cuánto son actualizados?

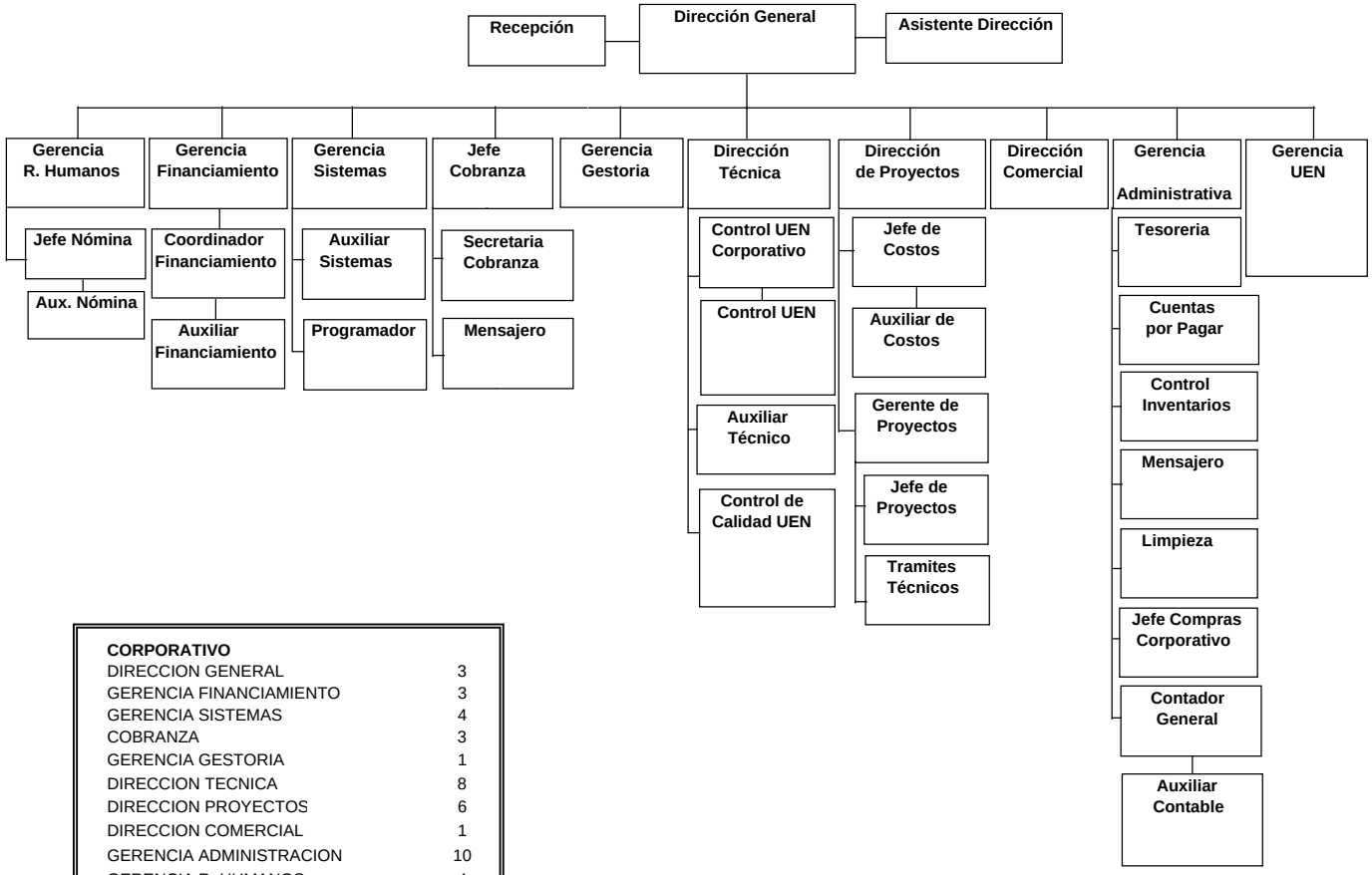
94. ¿Cómo controlan a los usuarios en lo que respecta a los virus?
95. ¿Qué proceso siguen en caso de que existan virus?
96. ¿Existe algún proceso que se siga para revisar la posible intrusión de virus?

Determinar si en el entorno ofimático se producen situaciones que pueden provocar infracciones.

97. ¿Se tiene una relación de todas las aplicaciones que precisen de licencias?
98. ¿Se tienen las licencias de todas las aplicaciones? ¿De cuáles sí y de cuáles no?
99. ¿Existen responsables de hacer una verificación periódica de las aplicaciones contenidas en los ordenadores y de analizar los niveles de utilización de las aplicaciones compartidas en la red?

ANEXO 1

ESTRUCTURA CORPORATIVO



CORPORATIVO	
DIRECCION GENERAL	3
GERENCIA FINANCIAMIENTO	3
GERENCIA SISTEMAS	4
COBRANZA	3
GERENCIA GESTORIA	1
DIRECCION TECNICA	8
DIRECCION PROYECTOS	6
DIRECCION COMERCIAL	1
GERENCIA ADMINISTRACION	10
GERENCIA R. HUMANOS	4
GERENCIA UEN	4
TOTAL	**47**

ANEXO 2

ORDEN DE COMPRA

PARA:	
COMPAÑÍA:	
FAX:	

DE:	
COMPAÑÍA:	
FAX:	

DEPARTAMENTO:		FECHA:
		PROVEDOR: 0
PLAZA:		**TELEFONO:**

DESCRIPCIÓN DEL ARTÍCULO	UNIDAD	CANTIDAD	P.U.	IMPORTE
				-

OBSERVACIONES:

SUBTOTAL	0.00
IVA	0.00
TOTAL	0.00

ELABORÓ **AUTORIZACIÓN**

NOTA: ENTREGAR EN OFICINA	
CON EL ENCARGADO:	

ANEXO 7

PERIFÉRICOS

DISPOSITIVO	MODELO	DEPARTAMENTO	NO. DE CONTROL	PLAZA
IMPRESORA	HP 1100	GESTORIA		OBREGON
IMPRESORA	HP 670C	VENTAS		OBREGON
IMPRESORA	HP 1120C	TECNICO		CORPORATIVO
IMPRESORA	HP 1100	FINANCIAMIENTO		CORPORATIVO
IMPRESORA	HP 2100	CONTRALORIA		CORPORATIVO
IMPRESORA	EPSON FX-880	NOMINAS		CORPORATIVO
IMPRESORA	EPSON FX-880	NOMINAS		CORPORATIVO
IMPRESORA	HP 930	ATENCION AL CLIENTE		OBREGON
IMPRESORA	HP 610	COMPRAS		OBREGON
IMPRESORA	HP 2100	ADMINISTRACION		CORPORATIVO
IMPRESORA	PANASONIC KX-P 3196	INVENTARIOS		OBREGON
IMPRESORA	EPSON FX-880	DESTAJOS		OBREGON
IMPRESORA	PANASONIC KX-P 3196	INVENTARIOS		NAVOJOA
IMPRESORA	EPSON FX-880	DESTAJOS		NAVOJOA
IMPRESORA	PANASONIC KX-P 3196	INVENTARIOS		NOGALES
IMPRESORA	EPSON FX-880	DESTAJOS		NOGALES
IMPRESORA	HP 830C	GESTORIA		NAVOJOA
IMPRESORA	HP 550C	CONTROL DE OBRA		NAVOJOA
IMPRESORA	HP 930	COMPRAS		NOGALES
IMPRESORA	HP 830C	GESTORIA		NOGALES
IMPRESORA	HP 1100	GESTORIA		NOGALES
IMPRESORA	HP 1100	GESTORIA		HERMOSILLO
IMPRESORA	HP 670C	COBRANZA INFONAVIT		CORPORATIVO
PLOTTER	HP 1050C	FINANCIAMIENTO		CORPORATIVO
SCANNER	HP 5200	FINANCIAMIENTO		CORPORATIVO

ANEXO 8

DEPARTAMENTO DE SISTEMAS
SOLICITUD DE SERVICIO

FECHA: _____

SISTEMA: _____

MODULO: _____

OPCION: _____

USUARIO: _____

ATENDIO: _____

DESCRIPCION DEL PROBLEMA:

MEDIDAS APLICADAS

_____ _____
USUARIO SISTEMAS