AUDITORIA DE SISTEMAS

****

**DISEÑAR UN LOGOTIPO PARA CONSULTORIA Y ADUITORIA ESTE ES SOLO UN EJEMPLO**

**AUDITORIA SALAS DE SISTEMAS**

**NOMBRE DE LA CORPORACION**

**AUDITORES**

**NOMBRE DEL (O LOS) INTEGRANTES**

**INTRODUCCION**

**CONCEPTO DE CALIDAD**

El término calidad es ambiguamente definido y pocas veces comprendido, esto se debe a que:

* La calidad no es una sola idea, es un concepto multidimensional;
* La dimensión de calidad incluye el interés de la entidad, el punto de vista de la entidad, y los atributos de la entidad;
* Por cada concepto existen diferentes niveles de abstracción;
* Varía para cada persona en particular.

Una definición que se podría dar de calidad sería:

*Conjunto de propiedades y de características de un producto o servicio, que*

*le confieren aptitud para satisfacer unas necesidades explícitas o implícitas.*

**Evolución Histórica**

Inspección/detección de errores: hasta los años 40.

Inicialmente el trabajo era artesanal y el control existente era individual, independiente de cada tarea.

En el año 1918, Ford Motor Company, monta la Primera cadena de montaje y en 1930 Laboratorios Bel la pone en marcha.

**Control (estadístico) de calidad: hasta los años 80.**

El mercado es poco competitivo. Precio de venta es fijado por el fabricante en función de los costes.

La principal función es impedir que el producto defectuoso llegue al cliente. Se persigue conseguir uniformidad de servicio.

El concepto de control de calidad es igual a “problema a resolver”. Se utilizan técnicas estadísticas para controlar la calidad del departamento de producción.

Se destacan en este periodo: Japón y Calidad total (1940-70). Deming,

Ishikawa, Juran, Crosby,…

**Garantía de calidad: a partir de los 80.**

El mercado se caracteriza por ser competitivo y de oferta. El precio de venta es fijado por el mercado. Entran en juego la planificación y medida de la calidad. Se implantan modelos de calidad que afectan a todos los departamentos.

1980. Interés por la calidad en los EEUU. TQM

1987. Premio *Malcom Baldrige Quality Award*

*1987.* ISO 9000. A partir de las normas británicas

1992. Premio Europeo a la calidad de la EFQM.

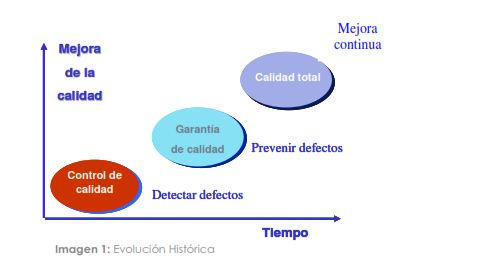
**Gestión de calidad hoy.**

Se busca un impacto estratégico y la oportunidad de ventaja competitiva.

Tienen relevancia conceptos como: Planificación, fijación de objetivos, coordinación, formación, adaptación de toda la organización.

La calidad afecta a la sociedad en general: directivos, trabajadores, clientes.

Se toma como “una filosofía, una cultura, una estrategia, un estilo de gerencia de la empresa”.



**Algunos conceptos**

**Calidad:** “Conjunto de propiedades y características de un producto o servicio que le confieren su aptitud para satisfacer unas necesidades explícitas o implícitas”

**Control de calidad:** “Conjunto de técnicas y actividades de carácter operativo, utilizadas para verificar los requerimientos relativos a la calidad del producto o servicio”.

**Garantía de calidad:** “Conjunto de acciones planificadas y sistemáticas necesarias para proporcionar la confianza adecuada de que un producto o servicio satisfará los requerimientos dados sobre calidad”.

**Gestión de la calidad:** “Aspecto de la función de gestión que determina y aplica la política de la calidad, los objetivos y las responsabilidades y que lo realiza con medios tales como la planificación de la calidad, el control de la calidad, la garantía de calidad y la mejora de la calidad”.

La gestión de la calidad es responsabilidad de todos los niveles ejecutivos, pero debe estar guiada por la alta dirección.

Su realización involucra a todos los miembros de la organización. En la gestión de la calidad, se tienen en cuenta también criterios de rentabilidad.

**Sistema de gestión de la calidad:** “Conjunto de la estructura de la organización, de responsabilidades, procedimientos, procesos y recursos que se establecen para llevar a término la gestión de calidad”. • Debe tener el volumen y alcance suficiente para conseguir los objetivos de calidad.

• Está fundamentalmente previsto para satisfacer las necesidades internas de la organización.).

• Para finalidades contractuales o vinculantes en la valoración de la calidad, se puede exigir que se ponga de manifiesto la realización de ciertos elementos del sistema de gestión de la calidad.

**Calidad del Software**

*“La calidad del software es el grado con el que un sistema, componente o proceso cumple los requerimientos especificados y las necesidades o expectativas del cliente o usuario”. (*IEEE, Std. 610-1990).

*“Concordancia del software producido con los requerimientos explícitamente establecidos, con los estándares de desarrollo prefijados y con los requerimientos implícitos no establecidos formalmente, que desea el usuario”* (Pressman, 1998).

* Factores que determinan la calidad del software:
* Se pueden clasificar en dos grandes grupos (Pressman):
* Factores que pueden ser medidos directamente.
* Factores que sólo pueden ser medidos indirectamente. Se centran en tres aspectos importantes de un producto software (McCall):
* Características operativas: Corrección, fiabilidad, eficiencia, seguridad (Integridad) y facilidad de uso.
* Capacidad de soportar los cambios: Facilidad de mantenimiento, flexibilidad y facilidad de prueba.
* Adaptabilidad a nuevos entornos: Portabilidad, reusabilidad e interoperabilidad.

**CONCEPTO DE SEGURIDAD**

**Seguridad de la Información**

La seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, disrupción o destrucción no autorizada.

Los términos Seguridad de Información, Seguridad informática y garantía de la información son usados con frecuencia y aunque su significado no es el mismo, persiguen una misma finalidad al proteger la Confidencialidad, Integridad y Disponibilidad de la información. Sin embargo, entre ellos existen algunas diferencias sutiles. Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración.

La Seguridad de la Información se refiere a la Confidencialidad, Integridad y Disponibilidad de la información y datos, independientemente de la forma que los datos puedan tener: electrónicos, impresos, audio u otras formas.

En caso de que la información confidencial de una empresa, sus clientes, sus decisiones, su estado financiero o la nueva línea de productos caigan en manos de un competidor o se vuelva pública en forma no autorizada, podría causar la pérdida de credibilidad de los clientes, pérdida de negocios, demandas legales o incluso la quiebra de la misma. Por lo que proteger la información confidencial es un requisito del negocio, y en muchos casos también un imperativo ético y una obligación legal.

Para el individuo común, la Seguridad de la Información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.

El campo de la Seguridad de la Información ha crecido y evolucionado considerablemente en los últimos años. Convirtiéndose en una carrera acreditada a nivel mundial. La misma ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, Planificación de la continuidad del negocio, Ciencia Forense Digital y Administración de Sistemas de Gestión de Seguridad por nombrar algunos.

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información.

**Confidencialidad:** La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

**Integridad:** Para la Seguridad de la Información, la integridad es la propiedad que busca mantener a los datos libres de modificaciones no autorizadas.

**Disponibilidad:** La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

**Seguridad Informática**

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

***Objetivos de la seguridad informática:***

Los activos son los elementos que la seguridad informática tiene como objetivo proteger. Son tres elementos que conforman los activos:

**Información:** Es el objeto de mayor valor para una organización. El objetivo es el resguardo de la información, independientemente del lugar en donde se encuentre registrada, en algún medio electrónico o físico.

**Equipos que la soportan**: Software, hardware y organización.

**Usuarios**: Individuos que utilizan la estructura tecnológica y de comunicaciones que manejan la información.

**INDICE DEL PROYECTO DE AUDITORIA DE SISTEMAS**

**CONSIDERACIONES PREVIAS**

Cada día son más las empresas que perciben su información como el motor del negocio que es, un activo estratégico que diariamente es sometido a nuevos y más graves riesgos imposibilitando que de manera efectiva, la información aporte el valor que tiene, siendo necesario vencer la inseguridad y la desconfianza que esto genera. Virus, hackers, averías, incendios, personal descontento, errores humanos, son miles las amenazas que tienen efectos devastadores, y que generan:

* Indisponibilidad: No poder acceder a la información cuando es vital y necesaria para la toma de decisiones, por inoperatividad de las infraestructuras tecnológicas.
* Falta de confidencialidad: Información accedida por personas no autorizadas. Robo de datos de clientes, espionaje, filtraciones, fraude.
* Pérdida de integridad: alteración de la información intencionada o por error al no existir controles.
* Falta de confianza en las transacciones electrónicas con terceros, al no existir mecanismos de autenticidad y repudio.

Afrontar estas situaciones, controlando la inseguridad de nuestros sistemas de información dentro de límites aceptables por el negocio sólo es posible mediante la integración de medidas organizativas y técnicas en el marco del desarrollo de una Cultura de la Seguridad y Calidad de la Información en la empresa.

No es posible eliminar las amenazas pero sí debemos reducir la posibilidad de que actúen y el perjuicio que pueden ocasionar: Es decir, controlar el riesgo para generar seguridad y confianza, aportando veracidad y calidad a la información que se está tratando.

En una sociedad en la que los cambios se producen de manera vertiginosa, y donde la información, la tecnología y su continua innovación son el propulsor principal de una espiral de oportunidades, nuevos riesgos amenazan permanentemente a las organizaciones: la complejidad de la tecnología, información de deficiente calidad, confidencialidad comprometida etc., cuyos efectos son cada vez más graves: pérdida de confianza y oportunidad, costes económicos...

Por ello es necesario proteger la información de las organizaciones y la confianza de sus clientes ayudando al desarrollo de una verdadera cultura de la seguridad en la empresa, desarrollar un proceso de mejora continua y maduración, a través de la evaluación, metodologías de calidad, la auditoría Informática y ayudar a las empresas en el cumplimiento de las normativas.

Actualmente todas las entidades que realizan software comienzan a prestar una gran atención en la calidad y seguridad de sus productos. Esto se debe, en parte, a que los clientes cada vez son más exigentes. Además, el no tener calidad y seguridad, implica la pérdida de clientes puesto que acudirán a aquellas empresas que les ofrezcan una calidad especificada por alguna norma y una seguridad a su producto.

La calidad pretende obtener el cumplimiento de las expectativas pactadas con el/los cliente/s siguiendo los estándares establecidos para garantizar así el éxito.

La calidad depende fundamentalmente de las expectativas de los clientes, ya que son ellos quienes finalmente perciben o evalúan la calidad. Bajo este prisma, la calidad puede ser definida como la brecha entre el desempeño real y el desempeño esperado. A menor brecha, mayor calidad.

Para lograr una buena calidad, es decir para que el desempeño del producto o servicio sea mayor o igual que las expectativas de los clientes, la clave está en conocer y comprender cuáles son esas expectativas.

El principal impacto de una mala calidad es la pérdida de rentabilidad y competitividad. Toda empresa que logra un buen nivel de calidad logra aumentar el valor de sus productos, sus ventas y su participación de mercado. Si además logra reducir sus costos, entonces la competitividad de la empresa será aún mayor.

Los datos de alta calidad deben ser completos, consistentes, exactos y actualizados. La necesidad de este tipo de datos es cada vez mayor ya que las compañías cada vez necesitan ser más eficientes en su operativa, cumplir con las normativas vigentes y contar con capacidades de monitorización que permitan que la calidad de datos se gestione como una iniciativa global.

La calidad comienza con una decisión estratégica que sólo puede ser tomada por la alta gerencia, la cual, es la decisión de competir como una compañía de categoría mundial. La calidad se concentra en lograr un desempeño de alta calidad en cada una de las facetas de la empresa.

La Seguridad informática no comprende únicamente características técnicas, sino que tiene que incorporar al personal, tanto interno como externo, a la gestión y a la organización.

Debido a la sensación de inseguridad que planea sobre la sociedad en general, también en el campo de la informática se requiere cada vez más un aumento de los niveles de Seguridad por parte de todos.

La Auditoría de Sistemas de Información comprende la revisión y la evaluación independiente y objetiva, abarcando todo o algunas de las áreas de los sistemas de información, sus estándares y procedimientos en vigor, para determinar si el sistema salvaguarda los activos, mantiene la integridad de la información y el cumplimiento de los objetivos fijados por la organización.

Teniendo en cuenta lo mencionado anteriormente, se puede observar la importancia de la Calidad y Seguridad en los entornos informáticos.

De esta importancia surge este proyecto, cuya finalidad es profundizar en el conocimiento de la calidad y de la seguridad de la información.

Se trata de relacionar ambas características, a la luz de los principales estándares aplicables, así como la auditoría como herramienta para las revisiones.

Se busca desarrollar una cultura de calidad y seguridad.

Se tratan los conceptos de calidad, seguridad y auditoría informática. La aplicación de estándares para su puesta en marcha y se dan detalles sobre su contenido. Con todo esto se pretende dar al lector un conocimiento más amplio de aquellas normas que afectan directamente a la calidad, a la seguridad y a la auditoría informática, que le permita saber que norma aplicar.

Se profundiza en estos conceptos, aplicándolos a las empresas y a la situación actual del mercado, evaluando las tendencias de la seguridad, auditoría y calidad en un futuro. Se puede observar la importancia de estos términos.

Además se le da gran importancia a la auditoría informática relacionada con la calidad y la seguridad.

El fin último es que cada persona implicada en labores informáticas esté convencida de que un trabajo bien hecho es aquel que cumple los requisitos de calidad y de seguridad necesarios, no sólo cuando ya está finalizado, sino durante toda su ejecución.

**Revisión Detallada**

* Pasos para la revisión detallada:

**A nivel organizacional.(ya lo obtuvieron de lA REVISION PRELIMINAR.)**

1. Objetivos a corto y largo plazo.
2. Misión, Visión y Valores.
3. Antecedentes de la empresa
4. Organigrama
5. Función de cada uno de los departamentos.
6. Relaciones entre las diversas áreas del negocio
7. Políticas Generales.

**A nivel del área de informática: (REVISION MAS DETALLADA DE ESTOS PUNTOS)**

1. Manual de Funciones (Fichas ocupacionales).
2. Manual de políticas, reglamentos internos y lineamientos generales.
3. Número de personas y puestos en el área.
4. Procedimientos administrativos del área.
5. Presupuestos y costos del área.

**RECURSOS MATERIALES Y TÉCNICOS: (REVISION MAS DETALLADA DE ESTOS PUNTOS)**

1. Solicitar documentos sobre los equipos, así como el número de ellos, su localización y sus características (de los equipos instalados, por instalar y programados).
2. Estudio de viabilidad.
3. Fechas de instalación de los equipos y planes de instalación.
4. Contratos vigentes de compra, renta y servicio de mantenimiento.
5. Contratos de seguros.
6. Convenios que se tienen con otras instalaciones.
7. Configuración de los equipos y capacidades actuales y máximas.
8. Configuración de equipos de comunicación(redes internas y externas) y localización de los equipos.
9. Planes de expansión.
10. Ubicación general de los equipos.
11. Políticas de operación.
12. Políticas del uso de los equipos.
13. Políticas de seguridad física y prevención contra contingencias internas y externas.

**sistemas: (REVISION MAS DETALLADA DE ESTOS PUNTOS)**

1. Descripción general de los sistemas instalados y de los que estén por instalarse.
2. Manual de procedimientos de los sistemas.
3. Descripción genérica.
4. Diagramas de entrada, archivos, salidas.
5. Fecha de instalación de los sistemas.
6. Proyecto de instalación de nuevos sistemas.
7. Bases de datos, propietarios de la información y usuarios de la misma.
8. Procedimientos y políticas en caso de desastre.
9. Sistemas propios y/0 legalidad de los mismos.

**Pruebas de Controles de los Usuarios**

**Analizar los controles establecidos y proponer otros controles**

**Pruebas Sustantivas**

1. Pruebas para identificar errores en el procesamiento o de falta de seguridad o confidencialidad.
2. Pruebas para asegura la calidad de los datos.
3. Pruebas para identificar la inconsistencia de los datos.
4. Pruebas para comparar con los datos o contadores físicos.
5. Confirmación de datos con fuentes externas.
6. Pruebas para confirmar la adecuada comunicación.
7. Pruebas para determinar la falta de seguridad.
8. Pruebas para determinar problemas de legalidad.

**Examen y Evaluación de la Información**

**EVALUACIÓN DE SISTEMAS**

La elaboración de sistemas debe ser evaluada con mucho detalle, para lo cual se debe revisar si existen realmente sistemas entrelazados como un todo o bien si existen programas aislados. Otro de los factores a evaluar es si existe un plan estratégico para la elaboración de los sistemas o si se están elaborados sin el adecuado señalamiento de prioridades y de objetivos.

El plan estratégico deberá establecer los servicios que se presentarán en un futuro contestando preguntas como las siguientes:

1. ¿Cuáles servicios se implementarán?
2. ¿Cuándo se pondrán a disposición de los usuarios?
3. ¿Qué características tendrán?
4. ¿Cuántos recursos se requerirán?

La estrategia de desarrollo deberá establecer las nuevas aplicaciones, recursos y la arquitectura en que estarán fundamentados:

1. ¿Qué aplicaciones serán desarrolladas y cuando?
2. ¿Qué tipo de archivos se utilizarán y cuando?
3. ¿Qué bases de datos serán utilizarán y cuando?
4. ¿Qué lenguajes se utilizarán y en que software?
5. ¿Qué tecnología será utilizada y cuando se implementará?
6. ¿Cuantos recursos se requerirán aproximadamente?
7. ¿Cuál es aproximadamente el monto de la inversión en hardware y software?

En lo referente a la consulta a los usuarios, el plan estratégico debe definir los requerimientos de información de la dependencia.

1. ¿Qué estudios van a ser realizados al respecto?
2. ¿Qué metodología se utilizará para dichos estudios?
3. ¿Quién administrará y realizará dichos estudios?

En el área de auditoría interna debe evaluarse cuál ha sido la participación del auditor y los controles establecidos.

Por último, el plan estratégico determina la planeación de los recursos.

1. ¿Contempla el plan estratégico las ventajas de la nueva tecnología?
2. ¿Cuál es la inversión requerida en servicios, desarrollo y consulta a los usuarios?

El proceso de planeación de sistemas deberá asegurarse de que todos los recursos requeridos estén claramente identificados en el plan de desarrollo de aplicaciones y datos. Estos recursos (hardware, software y comunicaciones) deberán ser compatibles con la arquitectura y la tecnología, conque se cuenta actualmente.

Los sistemas deben evaluarse de acuerdo con el ciclo de vida que normalmente siguen: requerimientos del usuario, estudio de factibilidad, diseño general, análisis, diseño lógico, desarrollo físico, pruebas, implementación, evaluación, modificaciones, instalación, mejoras. Y se vuelve nuevamente al ciclo inicial, el cual a su vez debe comenzar con el de factibilidad.

La primera etapa a evaluar del sistema es el estudio de factibilidad, el cual debe analizar si el sistema es factible de realizarse, cuál es su relación costo/beneficio y si es recomendable elaborarlo.

Se deberá solicitar el estudio de factibilidad de los diferentes sistemas que se encuentren en operación, así como los que estén en la fase de análisis para evaluar si se considera la disponibilidad y características del equipo, los sistemas operativos y lenguajes disponibles, la necesidad de los usuarios, las formas de utilización de los sistemas, el costo y los beneficios que reportará el sistema, el efecto que producirá en quienes lo usarán y el efecto que éstos tendrán sobre el sistema y la congruencia de los diferentes sistemas.

En el caso de sistemas que estén funcionando, se deberá comprobar si existe el estudio de factibilidad con los puntos señalados y compararse con la realidad con lo especificado en el estudio de factibilidad

Por ejemplo en un sistema que el estudio de factibilidad señaló determinado costo y una serie de beneficios de acuerdo con las necesidades del usuario, debemos comparar cual fue su costo real y evaluar si se satisficieron las necesidades indicadas como beneficios del sistema.

Para investigar el costo de un sistema se debe considerar, con una exactitud razonable, el costo de los programas, el uso de los equipos (compilaciones, programas, pruebas, paralelos), tiempo, personal y operación, cosa que en la práctica son costos directos, indirectos y de operación.

Los beneficios que justifiquen el desarrollo de un sistema pueden ser el ahorro en los costos de operación, la reducción del tiempo de proceso de un sistema. Mayor exactitud, mejor servicio, una mejoría en los procedimientos de control, mayor confiabilidad y seguridad.

**EVALUACIÓN DEL ANÁLISIS**

En esta etapa se evaluarán las políticas, procedimientos y normas que se tienen para llevar a cabo el análisis.

Se deberá evaluar la planeación de las aplicaciones que pueden provenir de tres fuentes principales:

1. La planeación estratégica: agrupadas las aplicaciones en conjuntos relacionados entre sí y no como programas aislados. Las aplicaciones deben comprender todos los sistemas que puedan ser desarrollados en la dependencia, independientemente de los recursos que impliquen su desarrollo y justificación en el momento de la planeación.
2. Los requerimientos de los usuarios.
3. El inventario de sistemas en proceso al recopilar la información de los cambios que han sido solicitados, sin importar si se efectuaron o se registraron.

La situación de una aplicación en dicho inventario puede ser alguna de las siguientes:

1. Planeada para ser desarrollada en el futuro.
2. En desarrollo.
3. En proceso, pero con modificaciones en desarrollo.
4. En proceso con problemas detectados.
5. En proceso sin problemas.
6. En proceso esporádicamente.

Nota: Se deberá documentar detalladamente la fuente que generó la necesidad de la aplicación. La primera parte será evaluar la forma en que se encuentran especificadas las políticas, los procedimientos y los estándares de análisis, si es que se cumplen y si son los adecuados para la dependencia.

Es importante revisar la situación en que se encuentran los manuales de análisis y si están acordes con las necesidades de la dependencia. En algunas ocasiones se tiene una microcomputadora, con sistemas sumamente sencillos y se solicita que se lleve a cabo una serie de análisis que después hay que plasmar en documentos señalados en los estándares, lo cual hace que esta fase sea muy compleja y costosa. Los sistemas y su documentación deben estar acordes con las características y necesidades de una dependencia específica.

Se debe evaluar la obtención de datos sobre la operación, flujo, nivel, jerarquía de la información que se tendrá a través del sistema. Se han de comparar los objetivos de los sistemas desarrollados con las operaciones actuales, para ver si el estudio de la ejecución deseada corresponde al actual.

La auditoría en sistemas debe evaluar los documentos y registros usados en la elaboración del sistema, así como todas las salidas y reportes, la descripción de las actividades de flujo de la información y de procedimientos, los archivos almacenados, su uso y su relación con otros archivos y sistemas, su frecuencia de acceso, su conservación, su seguridad y control, la documentación propuesta, las entradas y salidas del sistema y los documentos fuentes a usarse.

Con la información obtenida podemos contestar a las siguientes preguntas:

1. ¿Se está ejecutando en forma correcta y eficiente el proceso de información?
2. ¿Puede ser simplificado para mejorar su aprovechamiento?
3. ¿Se debe tener una mayor interacción con otros sistemas?
4. ¿Se tiene propuesto un adecuado control y seguridad sobre el sistema?
5. ¿Está en el análisis la documentación adecuada?

**EVALUACIÓN DEL DISEÑO LÓGICO DEL SISTEMA**

En esta etapa se deberán analizar las especificaciones del sistema.

¿Qué deberá hacer?, ¿Cómo lo deberá hacer?, ¿Secuencia y ocurrencia de los datos, el proceso y salida de reportes?

Una vez que hemos analizado estas partes, se deberá estudiar la participación que tuvo el usuario en la identificación del nuevo sistema, la participación de auditoría interna en el diseño de los controles y la determinación de los procedimientos de operación y decisión.

Al tener el análisis del diseño lógico del sistema debemos compararlo con lo que realmente se está obteniendo en la cual debemos evaluar lo planeado, cómo fue planeado y lo que realmente se está obteniendo.

Los puntos a evaluar son:

1. Entradas.
2. Salidas.
3. Procesos.
4. Especificaciones de datos.
5. Especificaciones de proceso.
6. Métodos de acceso.
7. Operaciones.
8. Manipulación de datos (antes y después del proceso electrónico de datos).
9. Proceso lógico necesario para producir informes.
10. Identificación de archivos, tamaño de los campos y registros.
11. Proceso en línea o lote y su justificación.
12. Frecuencia y volúmenes de operación.
13. Sistemas de seguridad.
14. Sistemas de control.
15. Responsables.
16. Número de usuarios.

Dentro del estudio de los sistemas en uso se deberá solicitar:

1. Manual del usuario.
2. Descripción de flujo de información y/o procesos.
3. Descripción y distribución de información.
4. Manual de formas.
5. Manual de reportes.
6. Lista de archivos y especificaciones.

Lo que se debe determinar en el sistema:

En el procedimiento:

1. ¿Quién hace, cuando y como?
2. ¿Qué formas se utilizan en el sistema?
3. ¿Son necesarias, se usan, están duplicadas?
4. ¿El número de copias es el adecuado?
5. ¿Existen puntos de control o faltan?

En la gráfica de flujo de información:

1. ¿Es fácil de usar?
2. ¿Es lógica?
3. ¿Se encontraron lagunas?
4. ¿Hay faltas de control?

En el diseño:

1. ¿Cómo se usará la herramienta de diseño si existe?
2. ¿Qué también se ajusta la herramienta al procedimiento?

**EVALUACIÓN DEL DESARROLLO DEL SISTEMA**

En esta etapa del sistema se deberán auditar los programas, su diseño, el leguaje utilizado, interconexión entre los programas y características del hardware empleado (total o parcial) para el desarrollo del sistema.Al evaluar un sistema de información se tendrá presente que todo sistema debe proporcionar información para planear, organizar y controlar de manera eficaz y oportuna, para reducir la duplicidad de datos y de reportes y obtener una mayor seguridad en la forma más económica posible. De ese modo contará con los mejores elementos para una adecuada toma de decisiones.Al tener un proceso distribuido, es preciso considerar la seguridad del movimiento de la información entre nodos. El proceso de planeación de sistemas debe definir la red óptima de comunicaciones, los tipos de mensajes requeridos, el trafico esperado en las líneas de comunicación y otros factores que afectan el diseño. Es importante considerar las variables que afectan a un sistema: ubicación en los niveles de la organización, el tamaño y los recursos que utiliza.Las características que deben evaluarse en los sistemas son:

1. Dinámicos (susceptibles de modificarse).
2. Estructurados (las interacciones de sus componentes o subsistemas deben actuar como un todo)
3. Integrados (un solo objetivo). En él habrá sistemas que puedan ser interrelacionados y no programas aislados.
4. Accesibles (que estén disponibles).
5. Necesarios (que se pruebe su utilización).
6. Comprensibles (que contengan todos los atributos).
7. Oportunos (que esté la información en el momento que se requiere).
8. Funcionales (que proporcionen la información adecuada a cada nivel).
9. Estándar (que la información tenga la misma interpretación en los distintos niveles).
10. Modulares (facilidad para ser expandidos o reducidos).
11. Jerárquicos (por niveles funcionales).
12. Seguros (que sólo las personas autorizadas tengan acceso).
13. Únicos (que no duplique información).

**CONTROL DE PROYECTOS**

Debido a las características propias del análisis y la programación, es muy frecuente que la implantación de los sistemas se retrase y se llegue a suceder que una persona lleva trabajando varios años dentro de un sistema o bien que se presenten irregularidades en las que los programadores se ponen a realizar actividades ajenas a la dirección de informática. Para poder controlar el avance de los sistemas, ya que ésta es una actividad de difícil evaluación, se recomienda que se utilice la técnica de administración por proyectos para su adecuado control.

Para tener una buena administración por proyectos se requiere que el analista o el programador y su jefe inmediato elaboren un plan de trabajo en el cual se especifiquen actividades, metas, personal participante y tiempos. Este plan debe ser revisado periódicamente (semanal, mensual, etc.) para evaluar el avance respecto a lo programado. La estructura estándar de la planeación de proyectos deberá incluir la facilidad de asignar fechas predefinidas de terminación de cada tarea. Dentro de estas fechas debe estar el calendario de reuniones de revisión, las cuales tendrán diferentes niveles de detalle.

CUESTIONARIO

1. ¿Existe una lista de proyectos de sistema de procedimiento de información y fechas programadas de implantación que puedan ser considerados como plan maestro?   
2. ¿Está relacionado el plan maestro con un plan general de desarrollo de la dependencia?   
3. ¿Ofrece el plan maestro la atención de solicitudes urgentes de los usuarios?   
4. ¿Asigna el plan maestro un porcentaje del tiempo total de producción al reproceso o fallas de equipo?   
5. Escribir la lista de proyectos a corto plazo y largo plazo.   
6. Escribir una lista de sistemas en proceso periodicidad y usuarios.   
7. ¿Quién autoriza los proyectos?   
8. ¿Cómo se asignan los recursos?   
9. ¿Cómo se estiman los tiempos de duración?   
10. ¿Quién interviene en la planeación de los proyectos?   
11. ¿Cómo se calcula el presupuesto del proyecto?   
12. ¿Qué técnicas se usan en el control de los proyectos?   
13. ¿Quién asigna las prioridades?   
14. ¿Cómo se asignan las prioridades?   
15. ¿Cómo se controla el avance del proyecto?   
16. ¿Con qué periodicidad se revisa el reporte de avance del proyecto?   
17. ¿Cómo se estima el rendimiento del personal?   
18. ¿Con que frecuencia se estiman los costos del proyecto para compararlo con lo presupuestado?   
19. ¿Qué acciones correctivas se toman en caso de desviaciones?   
20. ¿Qué pasos y técnicas siguen en la planeación y control de los proyectos?   
Enumérelos secuencialmente.   
( ) Determinación de los objetivos.   
( ) Señalamiento de las políticas.   
( ) Designación del funcionario responsable del proyecto.   
( ) Integración del grupo de trabajo.   
( ) Integración de un comité de decisiones.   
( ) Desarrollo de la investigación.   
( ) Documentación de la investigación.   
( ) Factibilidad de los sistemas.   
( ) Análisis y valuación de propuestas.   
( ) Selección de equipos.   
21. ¿Se llevan a cabo revisiones periódicas de los sistemas para determinar si aún cumplen con los objetivos para los cuales fueron diseñados?   
De análisis SÍ ( ) NO ( )   
De programación SÍ ( ) NO ( )   
Observaciones   
22. Incluir el plazo estimado de acuerdo con los proyectos que se tienen en que el departamento de informática podría satisfacer las necesidades de la dependencia, según la situación actual.

**CONTROL DE DISEÑO DE SISTEMAS Y PROGRAMACIÓN**

El objetivo es asegurarse de que el sistema funcione conforme a las especificaciones funcionales, a fin de que el usuario tenga la suficiente información para su manejo, operación y aceptación. Las revisiones se efectúan en forma paralela desde el análisis hasta la programación y sus objetivos son los siguientes:

ETAPA DE ANÁLISIS Identificar inexactitudes, ambigüedades y omisiones en las especificaciones.

ETAPA DE DISEÑO Descubrir errores, debilidades, omisiones antes de iniciar la codificación.

ETAPA DE PROGRAMACIÓN Buscar la claridad, modularidad y verificar con base en las especificaciones.

Esta actividad es muy importante ya que el costo de corregir errores es directamente proporcional al momento que se detectan: si se descubren en el momento de programación será más alto que si se detecta en la etapa de análisis. Esta función tiene una gran importancia en el ciclo de evaluación de aplicaciones de los sistemas de información y busca comprobar que la aplicación cumple las especificaciones del usuario, que se haya desarrollado dentro de lo presupuestado, que tenga los controles necesarios y que efectivamente cumpla con los objetivos y beneficios esperados.

El siguiente cuestionario se presenta como ejemplo para la evaluación del diseño y prueba de los sistemas:

1. ¿Quiénes intervienen al diseñar un sistema?

1. Usuario.
2. Analista.
3. Programadores.
4. Operadores.
5. Gerente de departamento.
6. Auditores internos.
7. Asesores.
8. Otros.

2. ¿Los analistas son también programadores?   
SÍ ( ) NO ( )

3. ¿Qué lenguaje o lenguajes conocen los analistas?

4. ¿Cuántos analistas hay y qué experiencia tienen?

5. ¿Qué lenguaje conocen los programadores?

6. ¿Cómo se controla el trabajo de los analistas?

7. ¿Cómo se controla el trabajo de los programadores?

8. Indique qué pasos siguen los programadores en el desarrollo de un programa:

1. Estudio de la definición ( )
2. Discusión con el analista ( )
3. Diagrama de bloques ( )
4. Tabla de decisiones ( )
5. Prueba de escritorio ( )
6. Codificación ( )
7. ¿Es enviado a captura o los programadores capturan? ( )
8. ¿Quién los captura?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
9. Compilación ( )
10. Elaborar datos de prueba ( )
11. Solicitar datos al analista ( )
12. Correr programas con datos ( )
13. Revisión de resultados ( )
14. Corrección del programa ( )
15. Documentar el programa ( )
16. Someter resultados de prueba ( )
17. Entrega del programa ( )

9. ¿Qué documentación acompaña al programa cuando se entrega?

Difícilmente se controla realmente el flujo de la información de un sistema que desde su inicio ha sido mal analizado, mal diseñado, mal programado e incluso mal documentado. El excesivo mantenimiento de los sistemas generalmente ocasionado por un mal desarrollo, se inicia desde que el usuario establece sus requerimientos (en ocasiones sin saber qué desea) hasta la instalación del mismo, sin que se haya establecido un plan de prueba del sistema para medir su grado de confiabilidad en la operación que efectuará. Para verificar si existe esta situación, se debe pedir a los analistas y a los programadores las actividades que están desarrollando en el momento de la auditoría y evaluar si están efectuando actividades de mantenimiento o de realización de nuevos proyectos. En ambos casos se deberá evaluar el tiempo que llevan dentro del mismo sistema, la prioridad que se le asignó y cómo está en el tiempo real en relación al tiempo estimado en el plan maestro.

**INSTRUCTIVOS DE OPERACIÓN**

Se debe evaluar los instructivos de operación de los sistemas para evitar que los programadores tengan acceso a los sistemas en operación, y el contenido mínimo de los instructivos de operación se puedan verificar mediante el siguiente cuestionario.

El instructivo de operación deberá comprender.

- Diagrama de flujo por cada programa. ( )   
- Diagrama particular de entrada/salida ( )   
- Mensaje y su explicación ( )   
- Parámetros y su explicación ( )   
- Diseño de impresión de resultados ( )   
- Cifras de control ( )   
- Fórmulas de verificación ( )   
- Observaciones ( )   
- Instrucciones en caso de error ( )   
- Calendario de proceso y resultados ( )

**FORMA DE IMPLEMENTACIÓN**

La finalidad de evaluar los trabajos que se realizan para iniciar la operación de un sistema, esto es, la prueba integral del sistema, adecuación, aceptación por parte del usuario, entrenamiento de los responsables del sistema etc.

Indicar cuáles puntos se toman en cuenta para la prueba de un sistema:

Prueba particular de cada programa ( )   
Prueba por fase validación, actualización ( )   
Prueba integral del paralelo ( )   
Prueba en paralelo sistema ( )   
Otros (especificar)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ENTREVISTA A USUARIOS**

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

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

Las entrevistas se deberán hacer, en caso de ser posible, a todos los usuarios o bien en forma aleatoria a algunos de los usuarios, tanto de los más importantes como de los de menor importancia, en cuanto al uso del equipo.

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

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

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

A continuación se presenta una guía de cuestionario para aplicarse durante la entrevista con el usuario.

1. ¿Considera que el Departamento de Sistemas de Información de los resultados esperados?.-   
Si ( ) No ( )   
¿Por que?

2. ¿Cómo considera usted, en general, el servicio proporcionado por el Departamento de Sistemas de Información?   
Deficiente ( )   
Aceptable ( )   
Satisfactorio ( )   
Excelente ( )   
¿Por que?

3. ¿Cubre sus necesidades el sistema que utiliza el departamento de cómputo?   
No las cubre ( )   
Parcialmente ( )   
La mayor parte ( )   
Todas ( )   
¿Por que?

4. ¿Hay disponibilidad del departamento de cómputo para sus requerimientos?   
Generalmente no existe ( )   
Hay ocasionalmente ( )   
Regularmente ( )   
Siempre ( )   
¿Por que?

5. ¿Son entregados con puntualidad los trabajos?   
Nunca ( )   
Rara vez ( )   
Ocasionalmente ( )   
Generalmente ( )   
Siempre ( )   
¿Por que?

6. ¿Que piensa de la presentación de los trabajadores solicitados al departamento de cómputo?   
Deficiente ( )   
Aceptable ( )   
Satisfactorio ( )   
Excelente ( )   
¿Por que?

7. ¿Que piensa de la asesoría que se imparte sobre informática?   
No se proporciona ( )   
Es insuficiente ( )   
Satisfactoria ( )   
Excelente ( )   
¿Por que?

8. ¿Que piensa de la seguridad en el manejo de la información proporcionada por el sistema que utiliza?   
Nula ( )   
Riesgosa ( )   
Satisfactoria ( )   
Excelente ( )   
Lo desconoce ( )   
¿Por que?

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

10. ¿Cómo utiliza los reportes que se le proporcionan?

11. ¿Cuáles no Utiliza?

12. De aquellos que no utiliza ¿por que razón los recibe?

13. ¿Que sugerencias presenta en cuanto a la eliminación de reportes modificación, fusión, división de reporte?

14. ¿Se cuenta con un manual de usuario por Sistema?   
SI ( ) NO ( )

15. ¿Es claro y objetivo el manual del usuario?   
SI ( ) NO ( )

16. ¿Que opinión tiene el manual?   
NOTA: Pida el manual del usuario para evaluarlo.

17. ¿Quién interviene de su departamento en el diseño de sistemas?

18. ¿Que sistemas desearía que se incluyeran?

19. Observaciones:

**CONTROLES**

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

a) La responsabilidad de los datos es compartida conjuntamente por alguna función determinada y el departamento de cómputo.

b) Un problema de dependencia que se debe considerar es el que se origina por la duplicidad de los datos y consiste en poder determinar los propietarios o usuarios posibles(principalmente en el caso de redes y banco de datos) y la responsabilidad de su actualización y consistencia.

c) Los datos deberán tener una clasificación estándar y un mecanismo de identificación que permita detectar duplicidad y redundancia dentro de una aplicación y de todas las aplicaciones en general.

d) Se deben relacionar los elementos de los datos con las bases de datos donde están almacenados, así como los reportes y grupos de procesos donde son generados.

***CONTROL DE LOS DATOS FUENTE Y MANEJO CIFRAS DE CONTROL***

La mayoría de los Delitos por computadora son cometidos por modificaciones de datos fuente al:

1. Suprimir u omitir datos.
2. Adicionar Datos.
3. Alterar datos.
4. Duplicar procesos.

Esto es de suma importancia en caso de equipos de cómputo que cuentan con sistemas en línea, en los que los usuarios son los responsables de la captura y modificación de la información al tener un adecuado control con señalamiento de responsables de los datos(uno de los usuarios debe ser el único responsable de determinado dato), con claves de acceso de acuerdo a niveles.

El primer nivel es el que puede hacer únicamente consultas. El segundo nivel es aquel que puede hacer captura, modificaciones y consultas y el tercer nivel es el que solo puede hacer todos lo anterior y además puede realizar bajas.

NOTA: Debido a que se denomina de diferentes formas la actividad de transcribir la información del dato fuente a la computadora, en el presente trabajo se le denominará captura o captación considerándola como sinónimo de digitalizar (capturista, digitalizadora).

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

1. Indique el porcentaje de datos que se reciben en el área de captación   
2. Indique el contenido de la orden de trabajo que se recibe en el área de captación de datos:   
Número de folio ( ) Número(s) de formato(s) ( )   
Fecha y hora de Nombre, Depto. ( )   
Recepción ( ) Usuario ( )   
Nombre del documento ( ) Nombre responsable ( )   
Volumen aproximado Clave de cargo   
de registro ( ) (Número de cuenta) ( )   
Número de registros ( ) Fecha y hora de entrega de   
Clave del capturista ( ) documentos y registros captados ( )   
Fecha estimada de entrega ( )

3. Indique cuál(es) control(es) interno(s) existe(n) en el área de captación de datos:   
Firmas de autorización ( )   
Recepción de trabajos ( ) Control de trabajos atrasados ( )   
Revisión del documento ( ) Avance de trabajos ( )   
fuente(legibilidad,   
verificación de datos   
completos, etc.) ( )   
Prioridades de captación ( ) Errores por trabajo ( )   
Producción de trabajo ( ) Corrección de errores ( )   
Producción de cada operador ( ) Entrega de trabajos ( )   
Verificación de cifras Costo Mensual por trabajo ( )   
de control de entrada con   
las de salida. ( )

4. ¿Existe un programa de trabajo de captación de datos?   
a) ¿Se elabora ese programa para cada turno?   
Diariamente ( )   
Semanalmente ( )   
Mensualmente ( )   
b) La elaboración del programa de trabajos se hace:   
Internamente ( )   
Se les señalan a los usuarios las prioridades ( )

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

5. ¿Quién controla las entradas de documentos fuente?

6. ¿En que forma las controla?

7. ¿Que cifras de control se obtienen?

Sistema Cifras que se Observaciones   
Obtienen

8. ¿Que documento de entrada se tienen?   
Sistemas Documentos Depto. que periodicidad Observaciones   
proporciona   
el documento

9. ¿Se anota que persona recibe la información y su volumen?   
SI NO

10. ¿Se anota a que capturista se entrega la información, el volumen y la hora?   
SI NO

11. ¿Se verifica la cantidad de la información recibida para su captura?   
SI NO

12. ¿Se revisan las cifras de control antes de enviarlas a captura?   
SI NO

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

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

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

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

17. ¿Existe un registro de anomalías en la información debido a mala codificación?

18. ¿Existe una relación completa de distribución de listados, en la cual se indiquen personas, secuencia y sistemas a los que pertenecen?

19. ¿Se verifica que las cifras de las validaciones concuerden con los documentos de entrada?

20. ¿Se hace una relación de cuando y a quién fueron distribuidos los listados?   
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

21. ¿Se controlan separadamente los documentos confidenciales?   
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

22. ¿Se aprovecha adecuadamente el papel de los listados inservibles?   
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

23. ¿Existe un registro de los documentos que entran a capturar?   
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

24. ¿Se hace un reporte diario, semanal o mensual de captura?   
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

25. ¿Se hace un reporte diario, semanal o mensual de anomalías en la información de entrada?

26. ¿Se lleva un control de la producción por persona?

27. ¿Quién revisa este control?

28. ¿Existen instrucciones escritas para capturar cada aplicación o, en su defecto existe una relación de programas?

***CONTROL DE OPERACIÓN***

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

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

1. ¿Existen procedimientos formales para la operación del sistema de computo?   
SI ( ) NO ( )

2. ¿Están actualizados los procedimientos?   
SI ( ) NO ( )

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

Semestral ( )   
Anual ( )   
Cada vez que haya cambio de equipo ( )

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

Identificación del sistema ( )   
Identificación del programa ( )   
Periodicidad y duración de la corrida ( )   
Especificación de formas especiales ( )   
Especificación de cintas de impresoras ( )   
Etiquetas de archivos de salida, nombre, ( )   
archivo lógico, y fechas de creación y expiración   
Instructivo sobre materiales de entrada y salida ( )   
Altos programados y la acciones requeridas ( )   
Instructivos específicos   
a los operadores en caso de falla del equipo ( )   
Instructivos de reinicio ( )   
Procedimientos de recuperación para proceso de   
gran duración o criterios ( )   
Identificación de todos los   
dispositivos de la máquina a ser usados ( )   
Especificaciones de resultados   
(cifras de control, registros de salida por archivo, etc. ) ( )

5. ¿Existen órdenes de proceso para cada corrida en la computadora (incluyendo pruebas, compilaciones y producción)?   
SI ( ) NO ( )

6. ¿Son suficientemente claras para los operadores estas órdenes?   
SI ( ) NO ( )

7. ¿Existe una estandarización de las ordenes de proceso?   
SI ( ) NO ( )

8. ¿Existe un control que asegure la justificación de los procesos en el computador? (Que los procesos que se están autorizados y tengan una razón de ser procesados.   
SI ( ) NO ( )

9. ¿Cómo programan los operadores los trabajos dentro del departamento de cómputo?   
Primero que entra, primero que sale ( )   
se respetan las prioridades, ( )   
Otra (especifique) ( )

10. ¿Los retrasos o incumplimiento con el programa de operación diaria, se revisa y analiza?   
SI ( ) NO ( )

11. ¿Quién revisa este reporte en su caso?

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

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

14. ¿Cómo se actúa en caso de errores?

15. ¿Existen instrucciones especificas para cada proceso, con las indicaciones pertinentes?

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

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

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

19. ¿Se prohibe al operador modificar información de archivos o bibliotecas de programas?

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

21. ¿Las intervenciones de los operadores:

Son muy numerosas? SI ( ) NO ( )   
Se limitan los mensajes esenciales? SI ( ) NO ( )   
Otras (especifique)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

22. ¿Se tiene un control adecuado sobre los sistemas y programas que están en operación?   
SI ( ) NO ( )   
23. ¿Cómo controlan los trabajos dentro del departamento de cómputo?

24. ¿Se rota al personal de control de información con los operadores procurando un entrenamiento cruzado y evitando la manipulación fraudulenta de datos?   
SI ( ) NO ( )

25. ¿Cuentan los operadores con una bitácora para mantener registros de cualquier evento y acción tomada por ellos?   
Si ( )   
por máquina ( )   
escrita manualmente ( )   
NO ( )   
26. Verificar que exista un registro de funcionamiento que muestre el tiempo de paros y mantenimiento o instalaciones de software.

27.¿Existen procedimientos para evitar las corridas de programas no autorizados?   
SI ( ) NO ( )

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

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

30. ¿Se hacen inspecciones periódicas de muestreo?   
SI ( ) NO ( )

31. Enuncie los procedimientos mencionados en el inciso anterior:

32. ¿Se permite a los operadores el acceso a los diagramas de flujo, programas fuente, etc. fuera del departamento de cómputo?   
SI ( ) NO ( )

33. ¿Se controla estrictamente el acceso a la documentación de programas o de aplicaciones rutinarias?   
SI ( ) NO ( )   
¿Cómo?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

35. ¿Existen procedimientos formales que se deban observar antes de que sean aceptados en operación, sistemas nuevos o modificaciones a los mismos?   
SI ( ) NO ( )

36. ¿Estos procedimientos incluyen corridas en paralelo de los sistemas modificados con las versiones anteriores?   
SI ( ) NO ( )

37. ¿Durante cuanto tiempo?

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

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

40. ¿Se catalogan los programas liberados para producción rutinaria?   
SI ( ) NO ( )

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

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

43. ¿Existe un lugar para archivar las bitácoras del sistema del equipo de cómputo?   
SI ( ) NO ( )

44. Indique como está organizado este archivo de bitácora.

1. Por fecha ( )
2. por fecha y hora ( )
3. por turno de operación ( )
4. Otros ( )

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

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

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

48. ¿Se tiene inventario actualizado de los equipos y terminales con su localización?   
SI ( ) NO ( )

49. ¿Cómo se controlan los procesos en línea?

50. ¿Se tienen seguros sobre todos los equipos?   
SI ( ) NO ( )

51. ¿Conque compañía?   
Solicitar pólizas de seguros y verificar tipo de seguro y montos.

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

***CONTROLES DE SALIDA***

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

2. ¿Dónde se encuentran esos locales?

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

4. ¿Que confidencialidad se tiene en esos locales?

5. ¿Quién entrega los documentos de salida?

6. ¿En que forma se entregan?

7. ¿Que documentos?

8. ¿Que controles se tienen?

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

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

Destruye ( ) Vende ( ) Tira ( ) Otro \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

***CONTROL DE MEDIOS DE ALMACENAMIENTO MASIVO***

Los dispositivos de almacenamiento representan, para cualquier centro de cómputo, archivos extremadamente importantes cuya pérdida parcial o total podría tener repercusiones muy serias, no sólo en la unidad de informática, sino en la dependencia de la cual se presta servicio. Una dirección de informática bien administrada debe tener perfectamente protegidos estos dispositivos de almacenamiento, además de mantener registros sistemáticos de la utilización de estos archivos, de modo que servirán de base a registros sistemáticos de la utilización de estos archivos, de modo que sirvan de base a los programas de limpieza (borrado de información), principalmente en el caso de las cintas.

Además se deben tener perfectamente identificados los carretes para reducir la posibilidad de utilización errónea o destrucción de la información.

Un manejo adecuado de estos dispositivos permitirá una operación más eficiente y segura, mejorando además los tiempos de procesos.

***CONTROL DE ALMACENAMIENTO MASIVO***

OBJETIVOS

El objetivo de este cuestionario es evaluar la forma como se administran los dispositivos de almacenamiento básico de la dirección.

1. Los locales asignados a la cintoteca y discoteca tienen:

1. Aire acondicionado ( )
2. Protección contra el fuego ( )
3. (señalar que tipo de protección )\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
4. Cerradura especial ( )
5. Otra

2. ¿Tienen la cintoteca y discoteca protección automática contra el fuego?   
SI ( ) NO ( )   
(señalar de que tipo)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. ¿Que información mínima contiene el inventario de la cintoteca y la discoteca?

Número de serie o carrete ( )   
Número o clave del usuario ( )   
Número del archivo lógico ( )   
Nombre del sistema que lo genera ( )   
Fecha de expiración del archivo ( )   
Fecha de expiración del archivo ( )   
Número de volumen ( )   
Otros

4. ¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos?   
SI ( ) NO ( )

5. En caso de existir discrepancia entre las cintas o discos y su contenido, se resuelven y explican satisfactoriamente las discrepancias?   
SI ( ) NO ( )

6. ¿Que tan frecuentes son estas discrepancias?   
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7. ¿Se tienen procedimientos que permitan la reconstrucción de un archivo en cinta a disco, el cual fue inadvertidamente destruido?   
SI ( ) NO ( )

8. ¿Se tienen identificados los archivos con información confidencial y se cuenta con claves de acceso?   
SI ( ) NO ( )   
¿Cómo?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

9. ¿Existe un control estricto de las copias de estos archivos?   
SI ( ) NO ( )

10. ¿Que medio se utiliza para almacenarlos?   
Mueble con cerradura ( )   
Bóveda ( )   
Otro(especifique)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

11. Este almacén esta situado:   
En el mismo edificio del departamento ( )   
En otro lugar ( )   
¿Cual?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

12. ¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos?   
SI ( ) NO ( )

13. ¿Se certifica la destrucción o baja de los archivos defectuosos?   
SI ( ) NO ( )   
14. ¿Se registran como parte del inventario las nuevas cintas que recibe la biblioteca?   
SI ( ) NO ( )

15 ¿Se tiene un responsable, por turno, de la cintoteca y discoteca?   
SI ( ) NO ( )

16. ¿Se realizan auditorías periódicas a los medios de almacenamiento?   
SI ( ) NO ( )

17. ¿Que medidas se toman en el caso de extravío de algún dispositivo de almacenamiento?

18. ¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, al personal autorizado?   
SI ( ) NO ( )

19. ¿Se tiene relación del personal autorizado para firmar la salida de archivos confidenciales?   
SI ( ) NO ( )

20. ¿Existe un procedimiento para registrar los archivos que se prestan y la fecha en que se devolverán?   
SI ( ) NO ( )

21. ¿Se lleva control sobre los archivos prestados por la instalación?   
SI ( ) NO ( )

22. En caso de préstamo ¿Conque información se documentan?   
Nombre de la institución a quién se hace el préstamo.

1. fecha de recepción ( )
2. fecha en que se debe devolver ( )
3. archivos que contiene ( )
4. formatos ( )
5. cifras de control ( )
6. código de grabación ( )
7. nombre del responsable que los presto ( )
8. otros

23. Indique qué procedimiento se sigue en el reemplazo de las cintas que contienen los archivos maestros:

24. ¿Se conserva la cinta maestra anterior hasta después de la nueva cinta?   
SI ( ) NO ( )

25. ¿El cintotecario controla la cinta maestra anterior previendo su uso incorrecto o su eliminación prematura?   
SI ( ) NO ( )

26. ¿La operación de reemplazo es controlada por el cintotecario?   
SI ( ) NO ( )

27. ¿Se utiliza la política de conservación de archivos hijo-padre-abuelo?   
SI ( ) NO ( )

28. En los procesos que manejan archivos en línea, ¿Existen procedimientos para recuperar los archivos?   
SI ( ) NO ( )

29. ¿Estos procedimientos los conocen los operadores?   
SI ( ) NO ( )

30. ¿Con que periodicidad se revisan estos procedimientos?   
MENSUAL ( ) ANUAL ( )   
SEMESTRAL ( ) OTRA ( )

31. ¿Existe un responsable en caso de falla?   
SI ( ) NO ( )

32. ¿Explique que políticas se siguen para la obtención de archivos de respaldo?

33. ¿Existe un procedimiento para el manejo de la información de la cintoteca?   
SI ( ) NO ( )

34. ¿Lo conoce y lo sigue el cintotecario?   
SI ( ) NO ( )

35. ¿Se distribuyen en forma periódica entre los jefes de sistemas y programación informes de archivos para que liberen los dispositivos de almacenamiento?   
SI ( ) NO ( )

¿Con qué frecuencia?

***CONTROL DE MANTENIMIENTO***

Como se sabe existen básicamente tres tipos de contrato de mantenimiento: El contrato de mantenimiento total que incluye el mantenimiento correctivo y preventivo, el cual a su vez puede dividirse en aquel que incluye las partes dentro del contrato y el que no incluye partes. El contrato que incluye refacciones es propiamente como un seguro, ya que en caso de descompostura el proveedor debe proporcionar las partes sin costo alguno. Este tipo de contrato es normalmente mas caro, pero se deja al proveedor la responsabilidad total del mantenimiento a excepción de daños por negligencia en la utilización del equipo. (Este tipo de mantenimiento normalmente se emplea en equipos grandes).

El segundo tipo de mantenimiento es “por llamada”, en el cual en caso de descompostura se le llama al proveedor y éste cobra de acuerdo a una tarifa y al tiempo que se requiera para componerlo(casi todos los proveedores incluyen, en la cotización de compostura, el tiempo de traslado de su oficina a donde se encuentre el equipo y viceversa). Este tipo de mantenimiento no incluye refacciones.

El tercer tipo de mantenimiento es el que se conoce como “en banco”, y es aquel en el cual el cliente lleva a las oficinas del proveedor el equipo, y este hace una cotización de acuerdo con el tiempo necesario para su compostura mas las refacciones (este tipo de mantenimiento puede ser el adecuado para computadoras personales).

Al evaluar el mantenimiento se debe primero analizar cual de los tres tipos es el que más nos conviene y en segundo lugar pedir los contratos y revisar con detalles que las cláusulas estén perfectamente definidas en las cuales se elimine toda la subjetividad y con penalización en caso de incumplimiento, para evitar contratos que sean parciales.

Para poder exigirle el cumplimiento del contrato de debe tener un estricto control sobre las fallas, frecuencia, y el tiempo de reparación.

Para evaluar el control que se tiene sobre el mantenimiento y las fallas se pueden utilizar los siguientes cuestionarios:

1. Especifique el tipo de contrato de mantenimiento que se tiene (solicitar copia del contrato).

2. ¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de computo?   
SI ( ) NO ( )

3. ¿Se lleva a cabo tal programa?   
SI ( ) NO ( )

4. ¿Existen tiempos de respuesta y de compostura estipulados en los contratos?   
SI ( ) NO ( )

5. Si los tiempos de reparación son superiores a los estipulados en el contrato, ¿Qué acciones correctivas se toman para ajustarlos a lo convenido?   
SI ( ) NO ( )

6. Solicite el plan de mantenimiento preventivo que debe ser proporcionado por el proveedor.-   
SI ( ) NO ( )   
¿Cual?

8. ¿Cómo se notifican las fallas?

9. ¿Cómo se les da seguimiento?

***ORDEN EN EL CENTRO DE CÓMPUTO***

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

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

Semanalmente ( ) Quincenalmente ( )   
Mensualmente ( ) Bimestralmente ( )   
No hay programa ( ) Otra (especifique) ( )

2. Existe un lugar asignado a las cintas y discos magnéticos?   
SI ( ) NO ( )

3. ¿Se tiene asignado un lugar especifico para papelería y utensilios de trabajo?   
SI ( ) NO ( )

4. ¿Son funcionales los muebles asignados para la cintoteca y discoteca?   
SI ( ) NO ( )

5. ¿Se tienen disposiciones para que se acomoden en su lugar correspondiente, después de su uso, las cintas, los discos magnéticos, la papelería, etc.?   
SI ( ) NO ( )

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

Al cambio de turno ( ) cada semana ( )   
cada día ( ) otra (especificar) ( )

7. ¿Existen prohibiciones para fumar, tomar alimentos y refrescos en el departamento de cómputo?   
SI ( ) NO ( )

8. ¿Se cuenta con carteles en lugares visibles que recuerdan dicha prohibición?   
SI ( ) NO ( )

9. ¿Se tiene restringida la operación del sistema de cómputo al personal especializado de la Dirección de Informática?   
SI ( ) NO ( )

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

**MODELOS DE CONTROL**

En la actualidad existen una gran cantidad de modelos de control interno.

Los modelos de control interno COSO y COBIT son los dos modelos más difundidos en la actualidad.

COSO está enfocado a toda la organización, contempla políticas, procedimientos y estructuras organizativas además de procesos para definir el modelo de control interno.

Mientras que COBIT (Control Objectives for Information and Related Technology, Objetivos de Control para Tecnología de Información y Tecnologías relacionadas) se centra en el entorno IT, contempla de forma específica la seguridad de la información como uno de sus objetivos, cosa que COSO no hace. Además el modelo de control interno que presenta COBIT es más completo, dentro de su ámbito.

Existen otros tipos de modelos los cuales se mencionan a continuación:

OECD (Organization for Economic Cooperation and Development)

GAPP (Generaly Accepted Principles and Practices). National Institute of Standards and Technology (NIST)

BS 7799 (British Standard Institute)

SAC (Security Auditability and Control). The Inst. of Internal Audit.

COSO (Internal Control Integrated Framework. Committee of Sponsoring Organizations)

SSE CMM (Systems Security Engineering Capability Maturity Model)

National Security Agency (NSA) Defense- Canada.

CoCo (Criteria of Control Board of The Canadian Instituteof Chartered Accountants.)

ITCG (Information Technology Control Guidelines). Canadian Institute of Chartered Accountants(CICA)

GASSP (Generaly Accepted System Security Principles). International

Information Security Foundation (IISF)

Cobit (Control Objectives for Information and Related Technologies) FISCAM (Federal Information Systems Controls Audit Manual).

GAO

SysTrust (AICPA/CICA SysTrust Principles and Criteria for System Reliability)

SSAG (System Self-Assessment Guide for Information Technology Systems). NIST

**COBIT – DEFINICIÓN**

Es un marco de control interno de TI.

Parte de la premisa de que la TI requiere proporcionar información para lograr los objetivos de la organización.

Promueve el enfoque y la propiedad de los procesos.

Apoya a la organización al proveer un marco que asegura que:

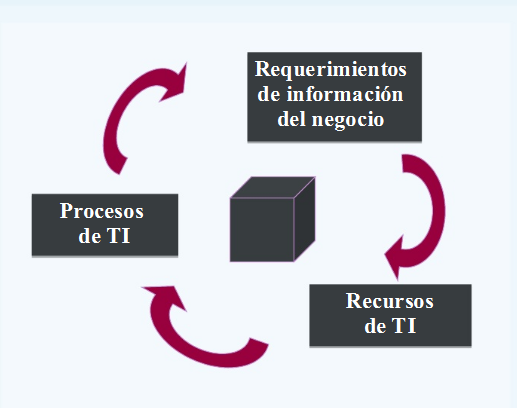
La Tecnología de Información (TI) esté alineada con la misión y visión.

LA TI capacite y maximice los beneficios.

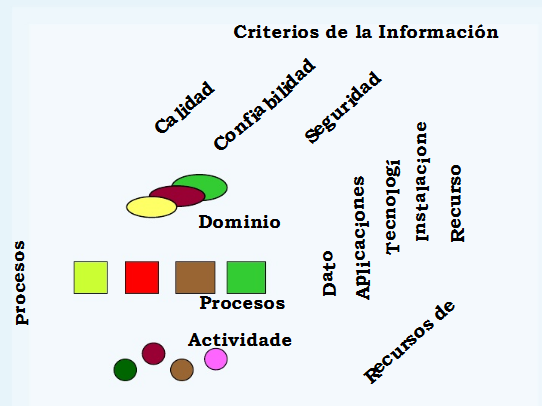
Los recursos de TI sean usados responsablemente.

Los riesgos de TI sean manejados apropiadamente.

COBIT – PRINCIPIOS

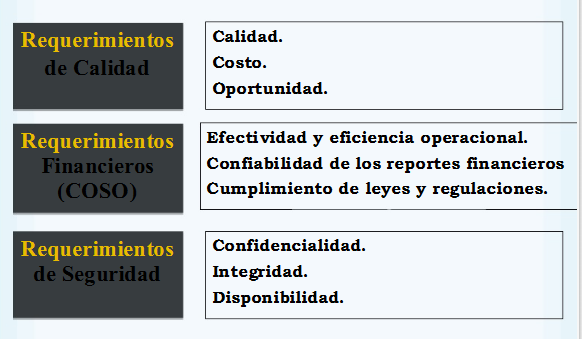


**COBIT – ESTRUCTURA**



COBIT – REQUERIMIENTOS DE LA INFORMACIÓN DEL NEGOCIO

COBIT combina los principios contenidos por modelos existentes y conocidos, como COSO, SAC Y SAS.



**COBIT – REQUERIMIENTOS DE LA INFORMACIÓN DEL NEGOCIO**

Efectividad: Información relevante y pertinente, proporcionada en forma oportuna, correcta, consistente y utilizable

Eficiencia: Empleo óptimo de los recursos.

Confidencialidad: Protección de la información sensitiva contra divulgación no autorizada

Integridad: Información exacta y completa, así como válida de acuerdo con las expectativas de la organización.

Disponibilidad: accesibilidad a la información y la salvaguarda de los recursos y sus capacidades.

Cumplimiento: Leyes, regulaciones y compromisos contractuales.

Confiabilidad: Apropiada para la toma de decisiones adecuadas y el cumplimiento normativo

**COBIT – PROCESOS DE TI – TRES NIVELES**



**1.1 Institución:**

**Logo:**

**Eslogan:**

**Direccion:**

**Ubicación:**

**Reseña Historica:**

**Web Site:**

**Filosofia Institucional:**

**1.2.Servicios que brinda:**

**1.3ÁREA INFORMÁTICA.**

La institución no cuenta con un área específica de informática, pero disponede una red de tipo estrella que esta en el área de administración u oficinaAdministrativa (OA) y esta constituida por 3 computadoras Pentium IV y unaPC portátil (Laptop

**AUDITORIA DE SISTEMAS**

**1.4. ORIGEN DE LA AUDITORIA**

La presente Auditoria se realiza en cumplimiento del Plan de Estudio que se tiene previsto para el periodo de Julio-Diciembre del 2011 el Centro Universitario Continental, aprobada mediante Plan de Estudios Auditoria al Procesamiento de Datos para la Licenciatura en Contaduría. Asesor Lic. Comp. Adriana Katia López Hernández

**1.5. OBJETIVOS Y ALCANCE**

**1.5.1 OBJETIVO GENERAL**

Revisar y Evaluar los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

**1.5.2 OBJETIVOS ESPECIFICOS**

Verificación del sistema eléctrico de la sala de informática.

Verificación de la comunicación interna y externa (Lan, Wan o Man)

Verificación de Licencias y sus tipos.

Verificación Perfiles del cargo (personal competente).

Verificación de los elementos del hardware.

Verificación del control de las normas en la sala de informática.

Verificación de los Planes de contingencia.

Verificación de la diagramación de la red.

Verificación de la seguridad inalámbrica.

**1.6. ENFOQUE A UTILIZAR**

La presente acción de control, Pero este artículo goza de su propio desarrollo reglamentario materializado en el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad., responsable de normar, supervisar y evaluar los métodos, procedimientos y técnicas estadísticas e informáticas, Normas Internacionales de Auditoria (NIA); habiéndose aplicado procedimientos de Auditoria que se consideraron necesarios de acuerdo a las circunstancias.

La presente Auditoria Informática se realizara en **NOMBRE DEL CASO DE ESTUDIO** siendo el área de Sistemas a examinarse.

**1.7. DOCUMENTOS A SOLICITAR**

* Políticas, estándares, normas y procedimientos**.(si no se tienen se manejan como propuestas)**
* Plan de sistemas. **.(si no se tienen se manejan como propuestas)**
* Planes de seguridad y continuidad**.(si no se tienen se manejan como propuestas)**
* Contratos, pólizas de seguros. **.(si no se tienen se manejan como propuestas)**
* Organigrama y manual de funciones. **.(si no se tienen se manejan como propuestas)**
* Manuales de sistemas. **.(si no se tienen se manejan como propuestas)**
* Registros**.(si no se tienen se manejan como propuestas)**
* Entrevistas**.(si no se tienen se manejan como propuestas)**
* Archivos**.(si no se tienen se manejan como propuestas)**
* Requerimientos de Usuarios**.(si no se tienen se manejan como propuestas)**

**1.8. ORGANIGRAMA**

Se tendrá el orden jerárquico que labora en CASO DE ESTUDIO.

**COLOCAR EL ORGANIGRAMA DE SUS CASOS DE ESTUDIO**

**1.9. RELACION DE FUNCIONARIOS DEL AREA A EXAMINAR**

Se relacionaran las personas que tienen relación con el Departamento de Sistemas de Acuerdo lo expresa el organigrama, teniendo en cuenta su cargo.

**DESCRIPCIÓN DE NOMBRES Y CARGOS.**

**1.10. TIPO DE SOFTWARE A UTILIZAR**

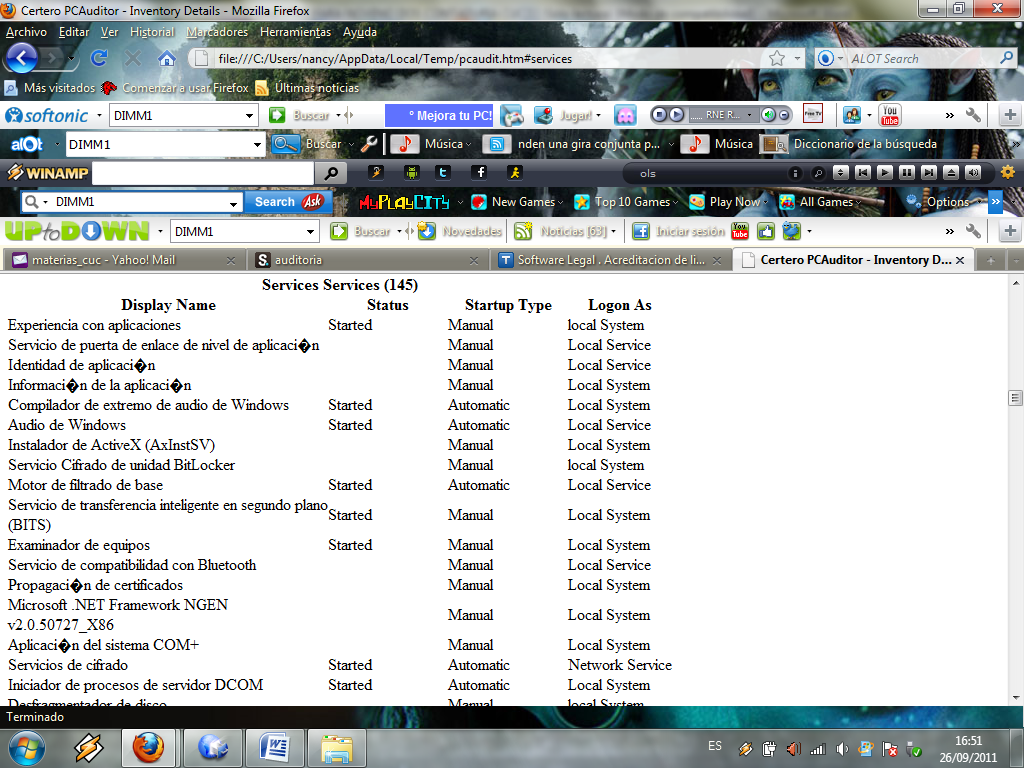
Se detallara el software utilizado para la verificación de licenciamiento del Software instalado en cada PC.

**1.7.1 CERTERO PCAUDITOR**

**HARDWARE**



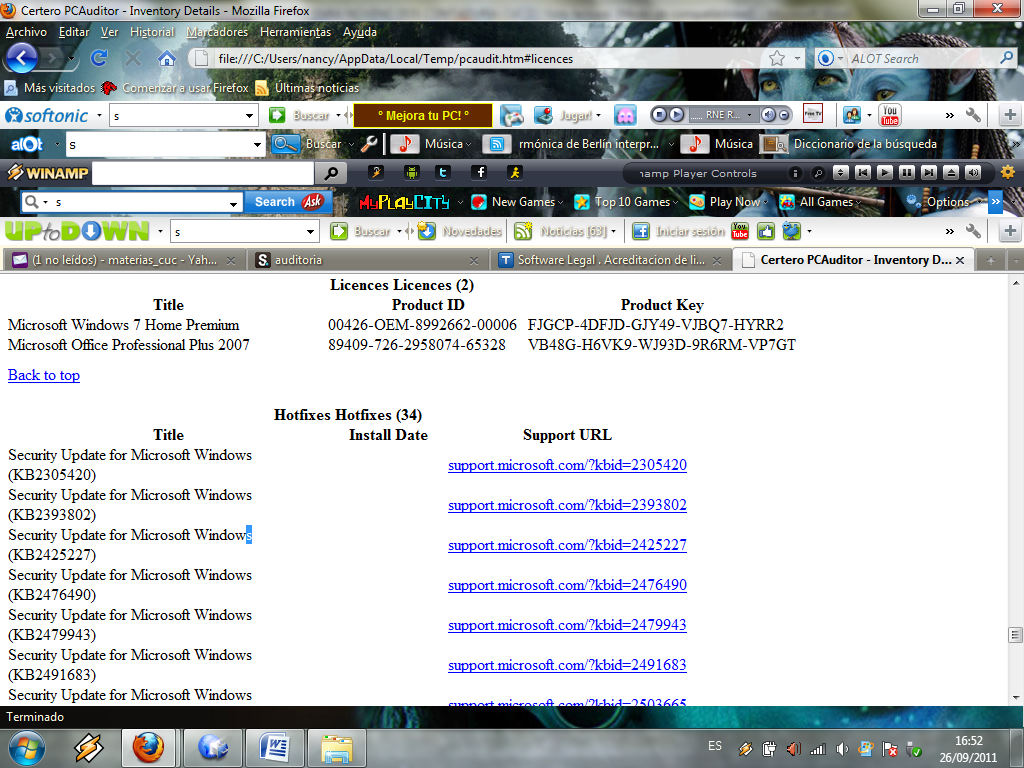
**SERVICES**

****

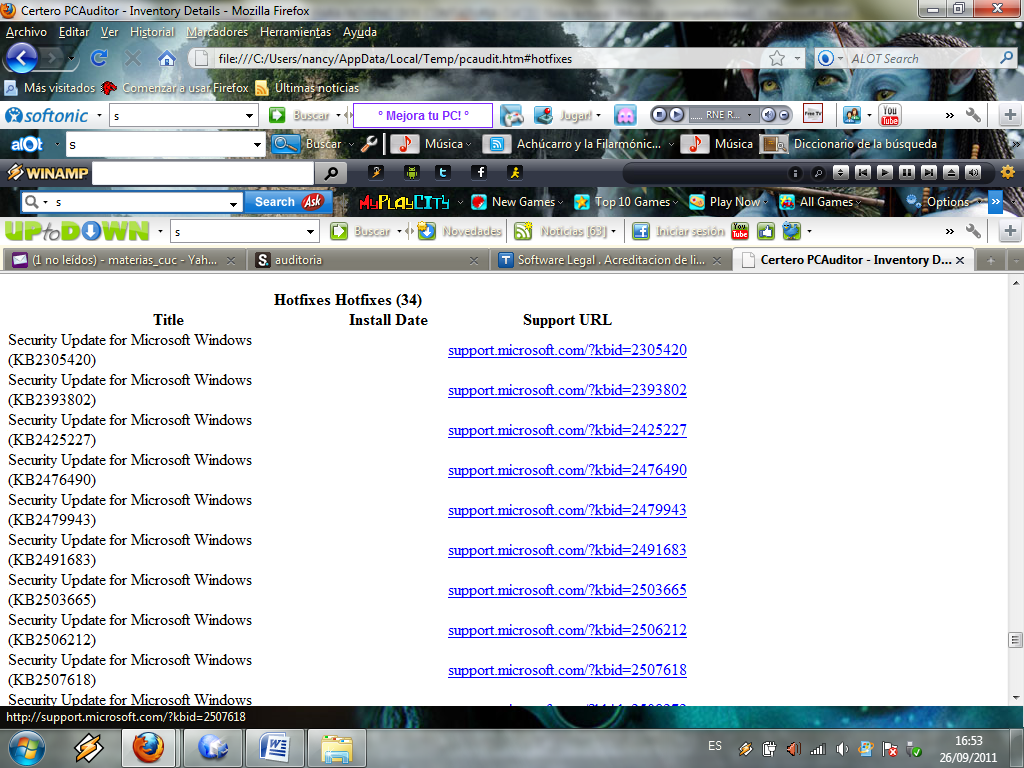
**SOFTWARE**

****

**LICENCIAS**

****

**SOPORTES**

****

**2. INFORMES**

Dentro del informe estamos tomando los siguientes puntos como referencia, para ser auditados.

* Equipos de cómputo y su ubicación.
* Las conexiones eléctricas de los equipos de cómputo.
* Cableado estructurado.
* Conexiones de redes.
* Licenciamiento de Software informático.
* Planes de contingencia.
* Normas implementadas en las salas de informática.

**El alcance de la auditoria nos mostrara si:**

* ¿Las condiciones de las salas de informática están acorde a las normas de
* seguridad industrial establecidas?
* ¿Los equipos de cómputo se encuentran en las condiciones mínimas requeridas
* para la prestación del servicio?
* ¿Las redes alambricas e inalámbricas se encuentran protegidas con contraseña,
* para evitar la intromisión de personal ajeno a la institución?
* ¿La ofimática de la sala se encuentra debidamente legalizada?
* ¿Las personas a cargo del mantenimiento de las salas, son idóneas y están
* capacitadas para dar respuesta oportuna a las necesidades de la misma?
* ¿Actualmente se encuentra con una diagramación de red a prueba de fallos?

A continuación expondremos la realidad de cada una de los puntos que se auditaron en las instalaciones **del caso de estudio** así:

**2.1. Equipos de Cómputo:**

Se cuenta **con numero de salas de informática**, las cuales serán auditadas de acuerdo a las normas que estén establecidas, se observará, y revisará de forma directa e indirecta los equipos, su instalación, ubicación y funcionamiento de las mismas.

Las cuales están bajo la responsabilidad **nombre y puesto del responsable**.

**2.1.1** **Cuantos equipos existen**

|  |  |
| --- | --- |
| **No de Monitores** | **No de CPU`s** |
|  |  |

**Características de conexión de los equipos en cuanto al cableado de cada uno.**

**Monitor**

**Torre**

**Mouse**

**Teclado**

**Ups**

**Reguladores de Voltaje**

**3. PUNTOS DEBILES Y AMENAZAS.**

**MATRIZ FODA(PROPUESTA)**

|  |  |
| --- | --- |
| FACTORES INTERNOS  Controlables | FACTORES EXTERNOS  No Controlables |
| **FORTALEZAS**    **(+)** | **OPORTUNIDADES**  **(+)** |
| **DEBILIDADES**  de los equipos de computo   * Estaciones de trabajo fuera de servicio. * Hacinamiento de las estaciones de trabajo. * Los recursos compartidos entre estaciones dificultan la interacción maquina estudiante, ya que el procesamiento de la información se pone lento. * No se realiza mantenimiento a las estaciones de trabajo periódicamente. * Establecer permisos para la instalación de programas y actualizaciones, esto evita la * entrada de virus que dañan los equipos.   (-) | **AMENAZAS**   * Posibilidad de daño en la torre administradora de las pantallas dejándolasinservibles. * La ubicación de la torre administradora no es la más adecuada. * Poca ventilación, lo que puede producir recalentamiento de las torres. * La posición de las pantallas no es la más adecuada. * El controlador de los dispositivos de teclado, mouse y red, puede fallar dejando * inutilizable la estación de trabajo. * Las estaciones de trabajo no cuentan con ningún tipo de código o serial que lo * pueda identificar como de la Corporación Universitaria, lo cual se puede prestar * para ser cambiadas por otras en mal estado.   (-) |

**3.1. RECOMENDACIONES DE LA AUDITORIA**

Después de analizar las diferentes amenazas que se presentan con los equipos de cómputo, los auditores hemos encontrado las siguientes recomendaciones:

* Ubicar los equipos de tal forma que no presenten un riesgo, tanto para el alumno como para la misma entidad.
* Lograr una mejor ventilación para los mismos, pues con la que cuentan actualmente, no se considera prudente.
* Un plan de contingencia ya que en el momento que una unidad conectora de dispositivos falle o en su defecto una torre, quedara inutilizable el resto de pantallas.
* De acuerdo con el crecimiento de la Corporación y del número de alumnos, se hace necesario estudiar la contratación ya sea por leasing o por compra empresarial de
* estaciones de trabajo completas y no dependientes.
* Dar una mejor ubicación a la torre administradora de las pantallas, pues es una máquina que esta propensa al daño no intencional por parte de algún alumno o de la misma persona de servicios generales.
* La numeración de las pantallas y las torres con un código de activo que permita su fácil identificación.

**4. CONEXIONES ELÉCTRICAS**

Después de recorrer las salas de cómputo, hemos podido detallar que no existe una correcta instalación eléctrica para los diferentes equipos y dispositivos que se manejan en las salas de sistemas.

La tendencia para este punto, es la certificación del cableado eléctrico **DEL CASO DE ESTUDIO.**

Para ello se pueden basar en la **Norma Técnica Colombiana NTC 2050A**, **INVESTIGAR** cuya primera actualización se publicó en 1.998 y está vigente.

**4.1. PUNTOS DÉBILES Y AMENAZAS.**

**Las debilidades que podemos encontrar con este tipo de cableado son:**

* **No hay garantía de funcionamiento permanente de las maquinas en el momento de un corto.**
* **Posibles sanciones para la corporación universitaria.**
* **Las amenazas que encontramos son las siguientes:**
* **Posibilidad de corto circuito.**
* **Daño temporal o permanente en las estaciones de trabajo.**
* **Daño en el software instalado en las maquinas por el apagado inesperado de la**
* **máquina.**
* **La imagen de la entidad se ve entredicho.**

**4.2. RECOMENDACIONES**

**Con base en la norma y en un plazo no muy largo, dar solucionar de fondo que garanticen el uso de una corriente certificada.**

**5. CABLEADO ESTRUCTURADO.**

Checar el cableado estructurado y fotografiarlo para así obtener evidencia de cómo se encontró. Evaluar si cumplen con normas.

## NORMA TIA/EIA-568-B

## Objetivos

TIA/EIA-568-B intenta definir estándares que permitirán el diseño e implementación de sistemas de cableado estructurado para edificios comerciales y entre edificios en entornos de campus. El sustrato de los estándares define los tipos de cables, distancias, conectores, arquitecturas, terminaciones de cables y características de rendimiento, requisitos de instalación de cable y métodos de pruebas de los cables instalados. El estándar principal, el TIA/EIA-568-B.1 define los requisitos generales, mientras que TIA/EIA-568-B.2 se centra en componentes de sistemas de cable de pares balanceados y el -568-B.3 aborda componentes de sistemas de cable de fibra óptica.

**5.1. PUNTOS DÉBILES Y AMENAZAS.**

Se hallan las siguientes amenazas:

* Es una mala imagen para la entidad no aplicar las normas.
* No existe garantía en el buen funcionamiento del cableado.

Las amenazas se pueden resumir en:

* Perdida de datos.
* Deficiencia en la comunicación entre equipos a nivel de red.

**5.2. RECOMENDACIONES**

Como auditores y basados en la norma mencionada en este documento, se le deja como recomendación, el estudio y la puesta en marcha de la instalación de el cableado estructurado.

Lo anterior con el fin de evitar gastos en pequeñas reparaciones, que con el tiempo van a significar un gran costo.

**6. CONEXIONES DE REDES**

Por las conexiones que presenta se puede determinar que el tipo de red está basado en una de área local.

Porque llegamos a esta conclusión:

* Existe un switch cuyo fin es interconectar conmutada las maquinas.
* Las máquinas están interconectadas a un único medio de comunicación.

Claro está que de una forma un poco rudimentaria sin llegar a tener un estándar de conexión bien definido.

La tendencia de la red de la corporación universitaria Remington, debe estar diseñada de una forma tal que se cumpla con el estándar y las normas de cableado estructurado y TCP IP.

**6.1. PUNTOS DÉBILES Y AMENAZAS**

Dentro de las debilidades de la red, podemos afirmar que no se tiene un tipo de red completamente definido, lo que hace imposible hallar una sola debilidad.

Las amenazas también son bastante grandes, pues no se cuenta medios de seguridad que no permita el acceso a la red de posibles hackers, o la llegada de software maligno, que al final logre el daño de las maquina o en un caso extremo de la red.

**Se realizará la propuesta de incluir para este punto los referente en el plan de seguridad.**

**7. LICENCIAMIENTO DEL SOFTWARE**

Este es un punto bastante crítico, para cualquier entidad en el país, ya que por ley las entidades o empresas legalmente constituidas en el país, no pueden contar con software ilegal o mal conocido como pirata en sus diferentes estaciones de trabajo.

Lo anterior de acuerdo a que el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 que obliga a las empresas a declarar si los problemas de software son o no legales.

Basados en lo anterior y consientes que la universidad no cuenta con el total de licencias para la legalidad de su software, se tiene como tendencia que en un corto Plazo este impase este resuelto.

**7.1. PUNTOS DÉBILES Y AMENAZAS**

**ESTO SE DEBIO OBTENER CON EL SOFTWARE QUE LES PROPORCIONE (CERTERO PC AUDITOR)**

La debilidad esta en no contar con un licenciamiento que le permita el uso legal del software que usa para el trabajo de sus estudiantes y planta física.

Además de incurrir en la violación a la ley que protege el derecho de autor, lo cual es sancionable.

Las siguientes son las amenazas a la que se expone la institución:

* Sanción económica y cierre de la institución.
* Procesos jurídicos a su representante legal.
* Mala imagen ante la comunidad educativa pues no está dando un ejemplo acorde a su misión que está basada en la formación integral de la persona con competencias profesionales, visión global y valores éticos, morales, políticos, económicos, ambientales y culturales.
* La imagen ante el estudiantado y la sociedad llanera.

**7.1.1. RECOMENDACIONES**

La recomendación que como auditores de la entidad podemos hacer es, la compra de las licencias o la instalación de software libre, el cual se puede conseguir a través de internet u otros medios y no generan costos.(**AUNQUE ESTO TENGA SUS LIMITANTES)**

**7.2. PLANES DE CONTINGENCIA.**

En los papeles de trabajo de la auditoria pudimos observar que no existe ningún tipo de plan o procedimiento, en el cual se de una contingencia a posibles daños en la estaciones de trabajo o en su información.

[*Plan de contingencia o de Seguridad (crearlo)*](file:///C:\Users\nancy\Documents\CUC\clases\clases%20Aud.proc.dat\EDITADOS\plan_seguridad.pdf)

**7.2.1. PUNTOS DÉBILES Y AMENAZAS.**

En este caso la debilidad está dada en no tener un modo de respaldar la información de carácter importante que hay en las estaciones de trabajo.

De igual forma es preocupante, no contar con unidades de cómputo que puedan reemplazar aquellas que por cualquier motivo queden fuera de servicio.

En lo que concierne a las amenazas podríamos destacar:

􀁸 No existe la forma de reemplazar las estaciones de trabajo en caso de daño.

􀁸 No hay un respaldo o un servidor donde se pueda almacenar la información de mayor importancia.

􀁸 En caso de daño de la red, no se cuenta con un proveedor certificado para una pronta solución.

Se debe tener en cuenta que la finalidad de este plan de contingencia es mantener el

funcionamiento de la corporación universitaria, sin que esta sufra traumatismo alguno

tecnológicamente.

**7.2.2. RECOMENDACIONES**

Lo más importante es evaluar el nivel de importancia de los datos que maneja la corporación universitaria y así iniciar la puesta en marcha del plan de contingencia adecuado.

**7.3. NORMAS PARA USO DE LAS SALAS DE SISTEMAS**

Después de realizar un recorrido por las diferentes salas de sistemas de la **NOMBRE DEL CASO DE ESTUDIO**, se pudo observar que muchos alumnos ingresan a las mismas con alimentos, sin control alguno.

También se puede ver que las salas no cuentan con señalización de evacuación, control sobre el hardware o software, ni ningún tipo de seguridad alguno.

*GENERAR UN REGLAMENTO DEL USO DE LOS EQUIPOS DE COMPUTO*

PROPUESTA

**Capítulo Primero**  
Definiciones para propósitos del presente reglamento

**Equipo computacional académico**Se considera como equipo computacional de uso académico a todo aquel equipo de cómputo, accesorio, periférico, de telecomunicaciones o relacionado con cualquiera de éstos, que esté instalado en las salas o laboratorios de acceso común administradas por la Dirección de Informática, además de los equipos instalados en las salas de cómputo centrales y que estén destinados al uso por parte de los usuarios académicos.

**Equipo computacional administrativo**Es todo aquel equipo adquirido por el Campus Monterrey o alguna de sus entidades y destinado a servir como apoyo a labores administrativas del personal del Campus. Dentro de esta categoría se considera el equipo instalado en las oficinas del Campus.

**Usuarios académicos**Se consideran usuarios académicos de los servicios de cómputo de la Dirección de Informática a:

* Los alumnos de la Rectoría de la Zona Metropolitana de Monterrey.
* Todos los profesores, profesionistas de apoyo y directivos del Sistema Tecnológico de Monterrey.
* Los alumnos de otros Campus del Sistema ITESM que se encuentren de visita, por motivos académicos, en nuestras instalaciones y se les haya autorizado a utilizarlas.

**Usuarios administrativos**Se consideran usuarios administrativos a:

* Los empleados, profesionistas de apoyo y directivos que hagan uso de los servicios de la Dirección de Informática como apoyo a sus actividades laborales.

**Uso académico**Se considera uso académico del equipo computacional y de comunicaciones a aquél que sirva como apoyo a la elaboración, solución, investigación de tareas, proyectos o trabajos relacionados directamente con cursos regulares impartidos en el Campus, así como el destinado a la preparación de material de apoyo a los mismos, y comunicación electrónica con otros usuarios académicos.

[Vuelve a inicio](http://publidinf.mty.itesm.mx/publidinfvirtual/reglamento/reglamento.htm#Inicio)

**Capítulo Segundo**  
Del uso de los equipos

El equipo computacional académico deberá utilizarse como herramienta de apoyo para labores académicas de los usuarios académicos, ya sea en las salas destinadas como recinto de este equipo, como a través de servicios de comunicación remota.

El uso del equipo computacional académico es exclusivo para los usuarios académicos. Cualquier persona que no esté considerada como tal y que desee hacer uso del equipo computacional académico deberá solicitar un permiso especial en la Dirección de Servicios Computacionales de la Dirección de Informática.

[Vuelve a inicio](http://publidinf.mty.itesm.mx/publidinfvirtual/reglamento/reglamento.htm#Inicio)

**Capítulo Tercero**Del acceso a las áreas de servicio computacional académico

Para tener acceso a las áreas de servicio computacional académico, se requiere que el interesado presente la credencial vigente que lo identifique como usuario académico a la persona encargada de vigilar la entrada a las salas de servicios computacionales.

Cuando el usuario sea alumno del Campus Monterrey, se podrá aceptar como identificación el comprobante de pago (Boleta de Pago) del período escolar en curso, con el sello de la Tesorería del ITESM y una identificación con fotografía. Esto se permite durante la primera semana del ciclo escolar.

El acceso a las áreas de servicio computacional académico será permitido de acuerdo a un horario que se publicará al inicio de cada semestre o cursos intensivos, y que se podrá consultar en cada una de estas áreas. En caso de presentarse modificaciones al mismo, se darán a conocer al menos con dos semanas de anticipación en cada una de las salas.

[Vuelve a inicio](http://publidinf.mty.itesm.mx/publidinfvirtual/reglamento/reglamento.htm#Inicio)

**Capítulo Cuarto**Del acceso a los servicios en equipos de cómputo centrales y servicios de red con autenticación

A todo profesor, profesionista de apoyo o directivo del Campus se le proporcionará, mediante solicitud, un identificador de acceso personalizado (cuenta) a los servicios de comunicación electrónica y de cómputo académicos o administrativos, según sea el caso, administrados por la Dirección de Informática.

A todos los alumnos se les proporcionará identificador único de acceso (cuenta) a los equipos de cómputo centrales con una configuración mínima que dependerá de la disponibilidad de recursos. En caso de que un alumno requiera una configuración diferente para uso académico, el profesor de la clase por la que él requiera este cambio deberá solicitarlo para el alumno por escrito.

Todas las cuentas irán acompañadas de una clave de acceso (password) que podrá ser cambiada a voluntad por el usuario.

Todas las cuentas deberán estar asociadas a un usuario, por lo que no se otorgarán cuentas para ser utilizadas por dos o más personas. Esto quiere decir, que las cuentas son personales e intransferibles.

El Campus Monterrey se reserva el derecho de suspender el servicio a un usuario cuando se sospeche de un abuso o uso indebido del servicio.

[Vuelve a inicio](http://publidinf.mty.itesm.mx/publidinfvirtual/reglamento/reglamento.htm#Inicio)

**Capítulo Quinto**Del comportamiento a observar

El comportamiento de todos los usuarios deberá ir de acuerdo a la moral y buenas costumbres.

Todo usuario deberá dar uso adecuado al equipo de cómputo, en el caso de que algún equipo resulte dañado por alguna acción atribuible al usuario, éste será acreedor a una sanción.

Cuando un usuario esté utilizando los servicios de comunicación electrónica, deberá observar las reglas que cada uno de estos servicios tenga dentro y fuera del Campus. En el caso de las redes internacionales el usuario será responsable de conocer y seguir las reglas que tenga la comunicación por este medio.

[Vuelve a inicio](http://publidinf.mty.itesm.mx/publidinfvirtual/reglamento/reglamento.htm#Inicio)

**Capítulo Sexto**De la separación de equipos o equipos con acceso restringido

Sólo se podrá restringir el acceso a un equipo si éste tiene facilidades de ser administrado en forma automática por medio de la asignación de claves.

Sólo podrá permitirse la separación de equipo en los siguientes casos:

* Cuando un profesor requiera que sus alumnos realicen una práctica relativa a su clase y supervisada por algún instructor, asesor o él mismo.
* Cuando la demanda por parte de los usuarios académicos sea tal, que sólo por medio de un esquema de reservación de equipos se consiga que más usuarios tengan acceso a los mismos.
* Cuando se trate de un equipo especial para el que se considere necesaria la separación desde el momento de su instalación en las salas.

Para solicitar la restricción de acceso o la separación de equipo es necesario que el profesor responsable haga una solicitud por escrito dirigida al Departamento de Servicios Computacionales.

El Departamento de Servicios Computacionales analizará todas las solicitudes relativas a la separación o restricción de acceso a los equipos y podrá dar curso a la solicitud de acuerdo a la disponibilidad de equipo y a la demanda del mismo por parte de los usuarios académicos. Con base en las consideraciones anteriores, se podrá revocar, previo aviso, la autorización para separar o restringir acceso a cualquier equipo.

En los periodos de alta demanda de los equipos computacionales académicos, éstos podrán ser sujetos a reservación. El tiempo máximo autorizado al que un usuario académico podrá ser autorizado para el uso de equipo computacional en una sesión, será determinado por el Departamento de Servicios Computacionales e informado en su oportunidad.

El usuario académico que haya reservado un equipo computacional para una sesión, podrá seguir utilizándolo por varias sesiones consecutivas de acuerdo a la disponibilidad de equipos, esto es, si hay equipos sin reservar.

Al momento de autorizarse la restricción de acceso a la separación de equipos, se definirán las reglas y procedimientos a seguir en su caso.

El usuario académico que haya reservado equipo con anticipación contará con 15 minutos de gracia para hacer uso de él, de lo contrario perderá su derecho a la reservación. Para la verificación de los tiempos, se utilizará el reloj oficial de área.

Todo usuario académico que abandone el equipo que esté utilizando por un período mayor a 15 minutos perderá el derecho a seguirlo utilizando si otro usuario lo demanda al encargado del área.

[Vuelve a inicio](http://publidinf.mty.itesm.mx/publidinfvirtual/reglamento/reglamento.htm#Inicio)

**Capítulo Séptimo**De las prohibiciones

Las actividades que se contemplan en este reglamento incluyen, pero no se limitan, a las siguientes restricciones; quedando prohibido a todos los usuarios:

* Introducir alimentos, bebidas o fumar en las áreas de servicio.
* Utilizar grabadoras, radios o equipos de sonido sin audífonos en las áreas de servicio.
* Utilizar los equipos computacionales académicos como máquinas de juegos; esto incluye utilizar software de juegos o acceder a servicios que impliquen el uso de juegos interactivos. De esta restricción se exceptúa el software de simulación autorizado para su uso por el Departamento de Servicios Computacionales bajo solicitud del profesor encargado de la materia en que se requiera.
* Utilizar el equipo computacional para desarrollar programas o proyectos ajenos al interés académico del Instituto.
* Extraer equipo computacional académico o sus partes de las áreas de servicio.
* Alterar o dañar las etiquetas de identificación de cualquier equipo computacional académico.
* Extraer materiales de consumo del equipo computacional académico o de las salas.
* Dejar material para utilizarse el siguiente día en las áreas de servicio o aulas activas.
* Copiar software cuya licencia de uso lo prohiba.
* Alterar software instalado en el equipo computacional académico.
* Utilizar el equipo computacional académico o la infraestructura de comunicación asociada a él para acceder equipos locales o remotos a los que el usuario no tenga autorización explícita, o en su uso, intentar violar la seguridad de acceso de cualquier equipo computacional.
* Utilizar claves de acceso o cuentas de otros usuarios o permitir a otros usuarios utilizar la propia.
* Interrumpir las labores de otros usuarios mediante mensajes, cuando éstos expresen su inconformidad.
* Utilizar una identidad diferente a la propia (de otro usuario o ficticia) o actuar en forma anónima para enviar mensajes en forma electrónica.
* Llevar a cabo acciones que interfieran o puedan interferir con la operación normal de los equipos computacionales o de comunicación electrónica del Campus o de cualquier instalación accesible desde el mismo.
* Utilizar los medios de comunicación electrónica de forma que puedan atentar contra otros individuos o interferir en sus actividades.
* Poseer información o llevar a cabo actividades que conduzcan o puedan conducir al uso no autorizado de información o recursos (computacionales o no) de cualquier institución dentro o fuera del Campus, ya sea por el usuario mismo u otras personas.
* Utilizar el equipo para actividades o aplicaciones diferentes a aquellas para las cuales el equipo está destinado (Equipos de uso especial).
* Utilizar los equipos instalados en las salas para desplegar material obsceno o que atente contra los valores que promueve el Instituto.
* Utilizar las áreas operativas del sistema para el almacenamiento de archivos personales.
* Intentar quebrantar las medidas de seguridad del sistema operativo.
* Compilar y ejecutar programas de dominio público cuya función sea intentar obtener privilegios mayores a los asignados.
* Enviar mensajes a otros usuarios de manera anónima.
* Conectar, desconectar o mover equipo computacional.

[Vuelve a inicio](http://publidinf.mty.itesm.mx/publidinfvirtual/reglamento/reglamento.htm#Inicio)

**Capítulo Octavo**De las sanciones

Toda violación a este reglamento será sancionada de acuerdo al Reglamento General de Alumnos del ITESM en el caso de los alumnos o por las autoridades correspondientes del Instituto en el caso del resto de los usuarios.

[Vuelve a inicio](http://publidinf.mty.itesm.mx/publidinfvirtual/reglamento/reglamento.htm#Inicio)

**Capítulo Noveno**De la confidencialidad de la información

Toda información almacenada en los equipos de cómputo central y no hecha explícitamente pública, será tratada como confidencial, y se harán todas las adecuaciones posibles por garantizar la privacidad de ésta.

En el caso de los equipos instalados en oficinas, será responsabilidad del usuario a quien fue asignado el tomar las medidas necesarias para proteger su información.

El Campus Monterrey, a través de la Rectoría del Campus y el departamento de Auditoría Interna se reservan el derecho de consultar la información almacenada en equipos propiedad del Campus cuando así lo juzguen conveniente ambas entidades.

La información administrativa y de administración académica contenida en los equipos del Instituto es privada y confidencial, y sólo deberán tener acceso a ella aquellos usuarios del Instituto que por sus funciones así lo requieran y sean autorizados.

El Instituto sólo podrá requerir el acceso a la información de un usuario cuando se presuma alguna falta que a juicio de las autoridades correspondientes del Campus, amerite lo anterior. Para esto se requiere la autorización, en el caso de los alumnos, de la Dirección de Asuntos Estudiantiles, y en el caso de otros usuarios, de la Rectoría del Campus Monterrey.

Todo usuario del cual se requiera consultar su información tendrá el derecho de estar presente en el momento de la consulta de la misma, que sólo podrá ser llevada a cabo, con la autorización respectiva y por escrito, por personal de la Dirección de Informática y de Auditoría Interna en conjunto.

[Vuelve a inicio](http://publidinf.mty.itesm.mx/publidinfvirtual/reglamento/reglamento.htm#Inicio)

**Capítulo Décimo**Observaciones Generales

La Dirección de Informática se reserva el derecho de utilizar los medios a su alcance para investigar posibles violaciones a este reglamento, siempre que sea respetada la confidencialidad de la información.

La Dirección de Informática se reserva el derecho de suspender o eliminar el acceso a cualquier equipo computacional a cualquier usuario, sin previo aviso al mismo, si el hacerlo es necesario para mantener la disponibilidad, seguridad e integridad de las operaciones para los demás usuarios de los recursos o del Campus Monterrey, o cuando se presuma alguna falta o violación a este reglamento u otros pertinentes que amerite este tipo de acciones para el proceso de investigación.

[Vuelve a inicio](http://publidinf.mty.itesm.mx/publidinfvirtual/reglamento/reglamento.htm#Inicio)

**Capítulo Undécimo**  
De la observancia y vigilancia del presente reglamento

Dada la naturaleza del presente reglamento, su conocimiento y observancia son obligatorios para todos los usuarios académicos del equipo computacional. Su desconocimiento nunca podrá ser invocado como excusa para evitar las sanciones correspondientes.

El presente reglamento entrará en vigor a partir de la fecha de su publicación y se revisará al inicio de cada semestre.

**7.3.1. PUNTOS DÉBILES Y AMENAZAS**

Son muchas las debilidades con las que cuentan las salas de cómputo caso de estudio entre ellas están:

* Falta de seguridad con el hardware.
* Consumo de alimentos.
* No hay control en la instalación de software.

Dentro de las amenazas se pueden encontrar:

* Daños a la infraestructura tecnológica.
* Hurto de los elementos de hardware.

**AUDITORIA FISICA**

**1. Alcance de la Auditoria**

* Organización y cualificación del personal de Seguridad.
* Remodelar el ambiente de trabajo.
* Planes y procedimientos.
* Sistemas técnicos de Seguridad y Protección.

**2. Objetivos**

* Revisión de las políticas y Normas sobre seguridad Física.
* Verificar la seguridad de personal, datos, hardware, software e instalaciones
* Seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático

|  |  |  |  |
| --- | --- | --- | --- |
| **PREGUNTAS** | **SI** | **NO** | **N/A** |
| 1. ¿Se han adoptado medidas de seguridad en el departamento de Sistemas? |  |  |  |
| 2. ¿Existe una persona responsable de la seguridad? |  |  |  |
| 3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad? |  |  |  |
| 4. ¿Existe personal de vigilancia en la institución? |  |  |  |
| 5. ¿Existe una clara definición de funciones entre los puestos clave? |  |  |  |
| 6. ¿Se investiga a los vigilantes cuando son contratados directamente? |  |  |  |
| 7. ¿Se controla el trabajo fuera de horario? |  |  |  |
| 8. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas? |  |  |  |
| 9. ¿Existe vigilancia en el departamento de cómputo las 24 horas? |  |  |  |
| 10. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores? |  |  |  |
| 11. ¿Se ha instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización? |  |  |  |
| 12. ¿El Departamento Sistemas y las salas tienen salida al exterior? |  |  |  |
| 13. ¿Son controladas las visitas y demostraciones a las salas de cómputo? |  |  |  |
| 14. ¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática? |  |  |  |
| 15. ¿Se vigilan la moral y comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar un posible fraude? |  |  |  |
| 16. ¿Se ha adiestrado el personal en el manejo de los extintores? |  |  |  |
| 17. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores? |  |  |  |
| 18. ¿Si es que existen extintores automáticos son activador por detectores automáticos de fuego? |  |  |  |
| 19. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos? |  |  |  |
| 20. ¿Saben que hacer los operadores del departamento de cómputo, encaso de que ocurra una emergencia ocasionado por fuego? |  |  |  |
| 21. ¿El personal ajeno a operación sabe qué hacer en el caso de una emergencia (incendio)? |  |  |  |
| 22. ¿Existe salida de emergencia? |  |  |  |
| 23. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen? |  |  |  |
| 24. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?  25. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo? |  |  |  |
| 26. ¿Se limpia con frecuencia el polvo acumulado debajo del piso falso si existe? |  |  |  |
| 27. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora? |  |  |  |
| 28. ¿Se tienen establecidos procedimientos de actualización a estas copias? |  |  |  |
| 29. ¿Existe departamento de auditoría interna en la institución? |  |  |  |
| 30. ¿El departamento de Sistemas conoce todos los aspectos de auditoría interna en los sistemas? |  |  |  |
| 31. ¿Se cumplen? |  |  |  |
| 32. ¿Se auditan los sistemas en operación? |  |  |  |

**Auditoria física:**

􀂙 **Para hallar el SI**

37 100%

10 X

**X = 27.03**

􀂙 **Para hallar el NO**

37 100%

15 X

**X = 40.54**

**LISTADO DE VERIFICACION DE AUDITORIA FISICA**

**Gestión Física de Seguridad**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| Los objetivos de la instalación física de computo |  |  |  |  |  |
| Las características físicas de las salas de sistemas son seguras |  |  |  |  |  |
| Los componentes físicos de computo |  |  |  |  |  |
| La conexiones de los equipos de las comunicaciones e instalaciones  físicas |  |  |  |  |  |
| La infraestructura es |  |  |  |  |  |
| El equipos es |  |  |  |  |  |
| La distribución de los quipos de computo es |  |  |  |  |  |

**Evaluación de análisis física de Cómputo**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| Evaluación de la existencia y uso de  normas, resolución base legal para el diseño del centro de cómputo. |  |  |  |  |  |
| El cumplimiento de los objetivos fundamentales de la organización para  instalar del centro de cómputo. |  |  |  |  |  |
| La forma de repartir los recursos informáticos de la organización |  |  |  |  |  |
| La confiabilidad y seguridades el uso de la  información institucional  La satisfacción de las necesidades de  poder computacional de la organización. |  |  |  |  |  |
| La solución a identificación del centro de cómputo (apoyó). |  |  |  |  |  |

**Análisis de la delimitación la manera en que se cumplen:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| La delimitación espacial, por las dimensiones  físicas. |  |  |  |  |  |
| La delimitación tecnológica, por los  requerimientos y conocimientos informáticos. |  |  |  |  |  |

**Análisis de la estabilidad y el aprovechamiento de los recursos a para instalar el centro de cómputo.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| Análisis de la transparencia del trabajo para los usuarios. |  |  |  |  |  |
| La ubicación del centro de computo |  |  |  |  |  |
| Los requerimientos de seguridad del centro  de computo |  |  |  |  |  |

**Evaluación del diseño según el ámbito**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| Análisis del ambiente de trabajo |  |  |  |  |  |
| Evaluar el funcionamiento de los equipos |  |  |  |  |  |
| El local para el trabajo es |  |  |  |  |  |
| Los equipos cuentan con ventilación |  |  |  |  |  |
| La iluminación **X** |  |  |  |  |  |

**Análisis de la seguridad física**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| La seguridad de los equipos. |  |  |  |  |  |
| El estado centro de computo esta |  |  |  |  |  |
| Los accesos de salida son |  |  |  |  |  |

**INFORME DE AUDITORIA**

**1. Identificación del informe**

Auditoria física.

**2. Identificación del Cliente**

Departamento De Sistemas, Salas de Computo

**3. Identificación de la Entidad Auditada**

**Caso de estudio**

**4. Objetivos**

* Verificar la estructura de distribución de los equipos.
* Revisar la correcta utilización de los equipos
* Verificar la condición del centro de cómputo.

**5. Hallazgos Potenciales**

* Falta de presupuesto y personal.
* Falta de un local más amplio.
* No existe un calendario de mantenimiento
* Falta de ventilación.
* Faltan salida al exterior
* No existe salidas de emergencia**.(CHECAR SI SE ENCONTRARON LOS MISMOS HALLAZGOS)**

**6. Alcance de la auditoria**

Nuestra auditoria, comprende el presente periodo 2011 y se ha realizado especialmente **al caso de estudio del área de**  de acuerdo a las normas y demás disposiciones aplicable al efecto.

El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoria Física, se complementa con los objetivos de ésta.

**7. Conclusiones:**

**Colocar cada una de las estrategias propuestas que emanan del análisis FODA.**

**8. Recomendaciones**

* **Reubicación de las salas de Informática**
* **Implantación de equipos de última generación**
* **Implantar equipos de ventilación**
* **Implantar salidas de emergencia.**
* **Elaborar un calendario de mantenimiento de rutina periódico.**
* **Capacitar al personal.**

**9. Fecha Del Informe**

**PLANEAMIENTO EJECUCION INFORME**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **PLANEAMIENTO** | **EJECUCIÓN** | **INFORME** |
| **FECHAS** | **01 DE AGOSTO AL 30 SEPTIEMBRE** | **01 DE OCTUBRE AL 01 DE NOVIEMBRE** | **16 DE NOVIEMBRE** |

**10. Identificación Y Firma Del Auditor**

|  |  |
| --- | --- |
| **APELLIDOS NOMBRES** | **CARGOS** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**AUDITORIA DE LA OFIMATICA**

**1. Alcance de la Auditoria.**

* Planes y procedimientos
* Políticas de Mantenimiento
* Inventarios Ofimáticos
* Capacitación del Personal

**2. Objetivos de la Auditoria.**

Realizar un informe de Auditoría con el objeto de verificar la existencia de controles

Preventivos, defectivos y correctivos, así como el cumplimiento de los mismos por los

usuarios.

|  |  |  |  |
| --- | --- | --- | --- |
| **PREGUNTAS** | **SI** | **NO** | **N/A** |
| 1. ¿Existe un informe técnico en el que se justifique la adquisición del equipo, software y servicios de Computación, incluyendo un estudio costo beneficio? |  |  |  |
| 2. ¿Existe un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación? |  |  |  |
| 3. ¿Han elaborado un instructivo con procedimientos a seguir para la selección y adquisición de equipos, programas y servicios computacionales? |  |  |  |
| 4. ¿se cuenta con software de oficina? |  |  |  |
| 5. ¿Se han efectuado las acciones necesarias para una mayor participación de proveedores? |  |  |  |
| 6. ¿Se ha asegurado un respaldo de mantenimiento y asistencia técnica? |  |  |  |
| 7. ¿El acceso al centro de cómputo cuenta con las seguridades necesarias para reservar el ingreso al personal autorizado? |  |  |  |
| 8. ¿Se han implantado claves o password para garantizar operación de consola y equipo central (mainframe), a personal autorizado? |  |  |  |
| 9. ¿Se han formulado políticas respecto a seguridad, privacidad y protección de las facilidades de procesamiento ante eventos como: incendio, vandalismo, robo y uso indebido, intentos de violación? |  |  |  |
| 10. ¿Se mantiene un registro permanente (bitácora) de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos? |  |  |  |
| 11. ¿Los operadores del equipo central están entrenados para recuperar o restaurar información en caso de destrucción de archivos? |  |  |  |
| 12. ¿Los backups son mayores de dos (padres e hijos) y se guardan en lugares seguros y adecuados, preferentemente en bóvedas de bancos? |  |  |  |
| 13. ¿Se han implantado calendarios de operación a fin de establecer prioridades de proceso? |  |  |  |
| 14. ¿Todas las actividades del Centro de Computo están normadas mediante manuales, instructivos, normas, reglamentos, etc.? |  |  |  |
| 15. ¿Las instalaciones cuentan con sistema de alarma por presencia de fuego, humo, así como extintores de incendio, conexiones eléctricas seguras entre otras |  |  |  |
| 16. ¿Se han instalado equipos que protejan la información y los dispositivos en caso de Variación de voltaje como: reguladores de voltaje, supresores pico, UPS,  generadores de energía? |  |  |  |
| 17. ¿Se han contratado pólizas de seguros para proteger la información, equipos, personal y todo riesgo que se produzca por casos fortuitos o mala operación? |  |  |  |
| 18. ¿Se han Adquirido equipos de protección como supresores de pico, reguladores de voltaje y de ser posible UPS previo a la adquisición del equipo? |  |  |  |
| 19. ¿Si se vence la garantía de mantenimiento del proveedor se contrata mantenimiento preventivo y correctivo? |  |  |  |
| 20. ¿Se establecen procedimientos para obtención de backups de paquetes y de archivos de datos? |  |  |  |
| 21. ¿Se hacen revisiones periódicas y sorpresivas del contenido del disco para verificar la instalación de aplicaciones no relacionadas a la gestión de la empresa? |  |  |  |
| 22. ¿Se mantiene programas y procedimientos de detección e inmunización de virus en copias no autorizadas o datos procesados en otros equipos? |  |  |  |
| 23. ¿Se propende a la estandarización del Sistema Operativo, software utilizado como procesadores de palabras, hojas electrónicas, manejadores de base de datos y se mantienen actualizadas las versiones y la capacitación sobre modificaciones incluidas? |  |  |  |
| 24. Existen licencias. |  |  |  |

**Auditoria Ofimática**

􀂙 **Para hallar el SI**

24 100%

7 X

**X = 29.17**

􀂙 **Para hallar el NO**

24 100%

13 X

**X = 54.17**

**INFORME DE AUDITORIA**

**1. Identificación del informe**

Auditoria de la Ofimática

**2. Identificación del Cliente**

**3. Identificación de la Entidad Auditada**

**4. Objetivos**

* Verificar si el hardware y software se adquieren siempre y cuando tengan la seguridad de que los sistemas computarizados proporcionaran mayores beneficios que cualquier otra alternativa.
* Verificar si la selección de equipos y sistemas de computación es adecuada
* Verificar la existencia de un plan de actividades previo a la instalación
* Verificar que los procesos de compra de Tecnología de Información, deben estar
* sustentados en Políticas, Procedimientos, Reglamentos y Normatividad en General, que aseguren que todo el proceso se realiza en un marco de legalidad y cumpliendo con las verdaderas necesidades de la organización para hoy y el futuro, sin caer en omisiones, excesos o incumplimientos.
* Verificar si existen garantías para proteger la integridad de los recursos informáticos.
* Verificar la utilización adecuada de equipos acorde a planes y objetivos.

**5. Hallazgos Potenciales**

􀂾 No tienen licencias de software.

􀂾 Falta de software de aplicaciones actualizados.

􀂾 No existe un calendario de mantenimiento ofimático.

􀂾 Faltan material ofimática.

􀂾 Falta de presupuesto.

􀂾 Carece de seguridad en Acceso restringido de los equipos ofimáticos y software.

**6. Alcance de la auditoria**

Nuestra auditoria, comprende el presente periodo 2011 y se ha realizado especialmente al

**CASO DE ESTUDIO** de acuerdo a las normas y demás disposiciones aplicable al efecto.

El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la

auditoria Ofimática, se complementa con los objetivos de ésta.

**7. Conclusiones:**

􀁸 Como resultado de la Auditoria podemos manifestar que hemos cumplido con evaluar

cada uno de los objetivos contenidos en el programa de auditoría.

􀁸 El Departamento de Sistemas y las salas de cómputo presenta deficiencias sobre el

debido cumplimiento de Normas de seguridad.

􀁸 La escasez de personal debidamente capacitado.

􀁸 Cabe destacar que los sistemas ofimáticos pudiera servir de gran apoyo a la

organización, el cual no es explotado en su totalidad por falta de personal capacitado.

**8. Recomendaciones**

􀁸 Se recomienda contar con sellos y firmas digitales.

􀁸 Un de manual de funciones y roles para cada puesto de trabajo dentro del área.

􀁸 Reactualización de datos.

􀁸 Adquisición de Licencias.

􀁸 Implantación de equipos de última generación.

􀁸 Elaborar un calendario de mantenimiento de rutina periódico.

􀁸 Capacitar al personal.

**9. Fecha Del Informe**

**PLANEAMIENTO EJECUCION INFORME**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **PLANEAMIENTO** | **EJECUCIÓN** | **INFORME** |
| **FECHAS** | **01 DE AGOSTO AL 30 SEPTIEMBRE** | **01 DE OCTUBRE AL 01 DE NOVIEMBRE** | **16 DE NOVIEMBRE** |

**10. Identificación Y Firma Del Auditor**

|  |  |
| --- | --- |
| **APELLIDOS NOMBRES** | **CARGOS** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**AUDITORIA A LOS SISTEMAS DE REDES**

**1. Alcance de la Auditoria.**

􀂾 Calificación del personal

􀂾 Sistemas técnicos de la red

􀂾 Mantenimiento de la Red

**2. Objetivos de la Auditoria.**

Realizar un informe de Auditoría con el objeto de verificar la adecuación de las medidas

aplicadas a las amenazas definidas, así como el cumplimiento de los requisitos exigidos.

**3. Referencia Legal.**

􀁸 Manual de Autoprotección aprobado por O.M. de 29/11/84, NBE-CPI 96 (RD 2177/96).

**4. Resultados.**

Se obtendrá:

􀁸 Informe de Auditoría detectando deficiencias en el Sistema de Redes.

􀁸 Plan de recomendaciones a aplicar en función de:

o Normativa a cumplir

o Recomendaciones

|  |  |  |  |
| --- | --- | --- | --- |
| **PREGUNTAS** | **SI** | **NO** | **N/A** |
| 1. El departamento de Sistemas tiene una política definida de planeamiento de tecnología de red? |  |  |  |
| 2. Esta política es acorde con el plan de calidad de la organización? |  |  |  |
| 3. El departamento de Sistemas tiene un plan que permite modificar en forma oportuna el plan a largo plazo de tecnología de redes, teniendo en cuenta los posibles cambios tecnológicos o en la organización? |  |  |  |
| 4. Existe un inventario de equipos y software asociados a las redes de Datos? |  |  |  |
| 5. Las redes de Datos se encuentran certificadas? |  |  |  |
| 6. Existe un plan de infraestructura de redes? |  |  |  |
| 7. El plan de compras de hardware y software para el sector redes está de acuerdo con el plan de infraestructura de redes? |  |  |  |
| 8. La responsabilidad operativa de las redes está separada de las de operaciones del computador? |  |  |  |
| 9. Están establecidos controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados |  |  |  |
| 10. Existen controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas? |  |  |  |
| 11. Existen controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red? |  |  |  |
| 12. Existen protocolos de comunicaron establecida |  |  |  |
| 13. Existe una topología estandarizada en toda la organización |  |  |  |
| 14. Existen normas que detallan que estándares que deben cumplir el hardware y el software de tecnología de redes?  15. ¿La transmisión de la información en las redes es segura? |  |  |  |
| 16. ¿El acceso a la red Wi-fi tiene password? |  |  |  |

**Auditoria de Redes:**

􀂙 **Para hallar el SI**

14 100%

5 X

**X = 35.71**

􀂙 **Para hallar el NO**

14 100%

9 X

**X = 64.29**

**AREA CRITICA REDES**

LISTADO DE VERIFICACIÓN DE AUDITORIA DE REDES

**Gestión Administrativa de la red.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| Los objetivos de la red de computo |  |  |  |  |  |
| Las características de la Red de computo |  |  |  |  |  |
| Los componentes físicos de la red de Computo |  |  |  |  |  |
| La conectividad y las Comunicaciones de la  red de computo |  |  |  |  |  |
| Los servicios que Proporcionan La red de  computo |  |  |  |  |  |
| Las configuraciones, topologías , tipos  Y cobertura de las redes de cómputo. |  |  |  |  |  |
| Los protocolos de Comunicación interna  de la red. |  |  |  |  |  |
| La administración de la red de Cómputo. |  |  |  |  |  |
| La seguridad de las redes de cómputo |  |  |  |  |  |

**Evaluación De Análisis De La Red De Cómputo**

Evaluar y calificar el cumplimiento de los siguientes aspectos:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| Evaluación de la existencia y uso de  metodologías, normas, estándares y  políticas para el análisis y diseño de redes  de cómputo. |  |  |  |  |  |
| Análisis de la definición de la problemática y  solución para instalar redes de cómputo en  la empresa. |  |  |  |  |  |
| Análisis de cumplimiento de los objetivos  fundamentales de la organización para  instalar una red de cómputo, evaluando en  cada caso. |  |  |  |  |  |
| La forma de repartir los recursos  informáticos de la organización,  especialmente la información y los activos |  |  |  |  |  |
| La cobertura de servicios informáticos para  la captura, el procesamiento y la emisión de  información en la organización |  |  |  |  |  |
| La cobertura de los servicios de comunicación. |  |  |  |  |  |
| La frecuencia con que los usuarios recurren  a los recursos de la red |  |  |  |  |  |
| La confiabilidad y seguridades el uso de la  información institucional. |  |  |  |  |  |
| La centralización , administración, operación  asignación y el control de los recursos informáticos de la organización. |  |  |  |  |  |
| La distribución equitativa de los costos de  adquisición y el control de los recursos  informáticos de la organización. |  |  |  |  |  |
| La escalabilidad y migración de los recursos  computacionales de la organización. |  |  |  |  |  |
| La satisfacción de las necesidades de poder  computacional de la organización ,sea con  redes ,cliente /servidor o mainframe |  |  |  |  |  |
| La solución a los problemas de  comunicación de información y datos en las  áreas de la organización |  |  |  |  |  |

**Análisis de los estudios de viabilidad y factibilidad en el diseño e instalación de la red de cómputo en la empresa:**

**Evaluar y calificar el cumplimiento de los siguientes aspectos**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| El estudio de factibilidad tecnológica |  |  |  |  |  |
| El estudio factibilidad económica |  |  |  |  |  |
| El estudio de factibilidad administrativa |  |  |  |  |  |
| El estudio de factibilidad operativa |  |  |  |  |  |

**Evaluación del diseño e implementación de la red según el ámbito de cobertura.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| Análisis de las redes de multi-computadoras |  |  |  |  |  |
| Evaluar el funcionamiento de la cobertura de punto a punto |  |  |  |  |  |
| Evaluar el funcionamiento de la tecnología que se usa con un solo cable entre las máquinas conectadas |  |  |  |  |  |
| Evaluar el funcionamiento de las aplicaciones, usos y explotación de las redes |  |  |  |  |  |

**Análisis de la red de área local (L A N).**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| Evaluar el uso adecuado y confiable de la  tecnología utilizada internamente para la  transmisión de datos |  |  |  |  |  |
| Evaluar la Restricción adoptada para  establecer el tamaño de la red |  |  |  |  |  |
| Evaluar la velocidad. |  |  |  |  |  |

**INFORME DE AUDITORIA**

**1. Identificación del informe**

Auditoria del Sistema de Redes

**2. Identificación del Cliente**

Departamento De Sistemas, Salas de Computo

**3. Identificación de la Entidad Auditada**

**4. Objetivos**

􀂾 Evaluar el tipo de red, arquitectura topología, protocolos de comunicación, las conexiones,

accesos privilegios, administración y demás aspectos que repercuten en su instalación.

􀂾 Revisión del software institucional para la administración de la red.

**5. Hallazgos Potenciales**

􀁸 No se cuenta con un Software que permita la seguridad de restricción y/o control a la Red.

􀁸 No existe un plan que asegure acciones correctivas asociadas a la conexión con redes

externas.

􀁸 No están definidos los parámetros o normas de calidad.

􀁸 El departamento de Sistemas no tiene un plan que permite modificar en forma oportuna el

plan a largo plazo de tecnología de redes, teniendo en cuenta los posibles cambios

tecnológicos.

􀁸 No existe un calendario de mantenimiento de rutina periódico del hardware definido por el

Departamento de Sistemas.

􀁸 No existe un plan proactivo de tareas a fin de anticipar los problemas y solucionarlos antes

de que los mismos afecten el desempeño de la red

**6. Alcance de la auditoria**

Nuestra auditoria, comprende el presente periodo 2011 y se ha realizado especialmente al

área de Informática de acuerdo a las normas y demás disposiciones aplicable al efecto.

**7. Conclusiones:**

􀁸 Como resultado de la Auditoria podemos manifestar que hemos cumplido con evaluar cada

uno de los objetivos contenidos en el programa de auditoría.

􀁸 El área de Informática presenta deficiencias sobre todo en el debido cumplimiento de

Normas de redes y funciones.

**8. Recomendaciones**

􀁸 Elaborar toda la documentación técnica correspondiente a los sistemas de redes.

􀁸 Evaluar e implementar un software que permita mantener el resguardo de acceso de los

archivos de programas.

􀁸 Implementar un plan que permita modificar en forma oportuna el plan a largo plazo de

tecnología de redes.

􀁸 Elaborar un calendario de mantenimiento de rutina periódico del hardware.

**9. Fecha Del Informe**

**PLANEAMIENTO EJECUCION INFORME**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **PLANEAMIENTO** | **EJECUCIÓN** | **INFORME** |
| **FECHAS** | **01 DE AGOSTO AL 30 SEPTIEMBRE** | **01 DE OCTUBRE AL 01 DE NOVIEMBRE** | **16 DE NOVIEMBRE** |

**10. Identificación Y Firma Del Auditor**

|  |  |
| --- | --- |
| **APELLIDOS NOMBRES** | **CARGOS** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**BALANCE DE RESULTADOS**

|  |  |  |
| --- | --- | --- |
| **AUDITORIA** | **SI** | **NO** |
| **FISICA** |  |  |
| **OFIMATICA** |  |  |
| **REDES** |  |  |

**CONCLUSIONES**

La principal conclusión a la que hemos podido llegar, es que toda empresa, pública o privada, que posean Sistemas de Información medianamente complejos, deben de someterse a un control estricto de evaluación de eficacia y eficiencia. Hoy en día, el 90 por ciento de las empresas tienen toda su información estructurada en Sistemas Informáticos, de aquí, la vital importancia que los sistemas de información funcionen correctamente. La empresa hoy, debe/precisa informatizarse.

El éxito de una empresa depende de la eficiencia de sus sistemas de información. Una empresa puede tener un staff de gente de primera, pero tiene un sistema informático propenso a errores, lento, vulnerable e inestable; si no hay un balance entre estas dos cosas, la empresa nunca saldrá a adelante. En cuanto al trabajo de la auditoria en sí, podemos remarcar que se precisa de gran conocimiento de Informática, seriedad, capacidad, minuciosidad y responsabilidad; la auditoria de Sistemas debe hacerse por gente altamente capacitada, una auditoria mal hecha puede acarrear consecuencias drásticas para la empresa auditada, principalmente económicas.

**INFORME FINAL DE AUDITORIA**

**La presente Auditoría ha sido solicitada por la Alta Dirección, quien aprobó los objetivos y alcance de la misma. Por lo anterior, se reconoce a ésta como cliente de la misma.**

**Objetivos**

* **Verificar la eficacia y eficiencia de los procesos y procedimientos asociados a las actividades diariamente realizadas por el personal participante.**
* **Localizar las oportunidades de mejora, para algunos procesos.**

**¿Cómo se auditó?**

* **Con la participación de personas auditores certificados y como auditor Lider**
* **Mediante entrevistas, encuestas y revisión documental se verificó el cumplimiento de los criterios de la auditoría en los procesos y áreas bajo alcance de la misma.**

**RESULTADOS**

* CASO DE ESTUDIO cuenta con la siguiente documentación:
* Carece de la siguiente información
* De la información que se careceré, se elaborara y se implementara de la siguiente forma:

|  |  |  |  |
| --- | --- | --- | --- |
| TIPO DE DOCUMENTO | RESPONSABLE | FECHA ESTIMADA ELABORACION | FECHA ESTIMADA DE IMPLEMENTACIÓN |
| PLAN DE CONTINGENCIA | DIRECTOR DEL DEPARTAMENTO DE INFORMATICA | 6 MESES | 1 AÑO |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

* El personal entrevistado demostró interés en trabajar utilizando las normas de Auditoria correspondientes.
* El personal mostró interés en iniciar los trabajos para evaluar el desempeño de sus procesos, en seguir otorgando los servicios y productos que por su experiencia está comprometido a realizar.
* Se confirma el compromiso y la oportunidad de avanzar hacia la mejora continua en la organización.
* La Alta Dirección tiene identificado los Objetivos de Calidad e indicadores institucionales.

**RESUMEN DE NO CONFORMIDADES**

|  |  |  |
| --- | --- | --- |
| **NO.** | **TIPO DE HALLAZGO** | **DESCRIPCIÓN DEL HALLAZGO** |
| 1 | **No Conformidad Mayor:**  **No hay o no se conocen los criterios para análisis medición y seguimiento de los resultados y operación de Procesos. REINCIDENTE EN LA AU-O4 PUNTO 7.5 DE LA NORMA** | * No se encuentra evidencia documental de que se realice la evaluación del desempeño de los procesos. Ejemplo: “Proyecto CITEQ, según la Bitácora del CEN”, “Laboratorio de Análisis de aguas de abastecimiento y residuales, según la bitácora del CEN”. * No se encuentra evidencia documental de que se realice la evaluación de la realización de los productos. Ejemplos: Proyecto de evaluación de poliquetas como degradadores de sedimentos contaminados.(DCI) |

**AREAS DE OPORTUNIDAD O DE MEJORA**

EN BASE A LAS AUDITORIAS ARRIBA REALIZADAS PLANTEAR LAS OPORTUNIDADES DE MEJORA.