UNIREMINGTON®
CORPORACIÓN UNIVERSITARIA REMINGTON
RES. 2661 MEN JUNIO 21 DE 1996

CONTROL DE INFORMÁTICA

ESPECIALIZACIÓN EN REVISORÍA FISCAL Y CONTRALORÍA

FACULTAD DE CIENCIAS CONTABLES

Vicerrectoría de Educación a Distancia y virtual

2016

AUTOR

Enevis Rafael Reyes Moreno
Ingeniero de sistemas con especialización en ciencias electrónicas e informáticas (Telemática). Docente universitario de pregrado de Ing. de Sistemas (ITM) y en especialización. En el área de informática, redes y auditoría. (REMINGTON, CONAAES)
enevisr@gmail.com

Nota: el autor certificó (de manera verbal o escrita) No haber incurrido en fraude científico, plagio o vicios de autoría; en caso contrario eximió de toda responsabilidad a la Corporación Universitaria Remington, y se declaró como el único responsable.

RESPONSABLES

Jorge Alcides Quintero Quintero
Decano de la Facultad de Ciencias Contables
jquintero@uniremington.edu.co

Eduardo Alfredo Castillo Builes
Vicerrector modalidad distancia y virtual
ecastillo@uniremington.edu.co

Francisco Javier Álvarez Gómez
Coordinador CUR-Virtual
falvarez@uniremington.edu.co

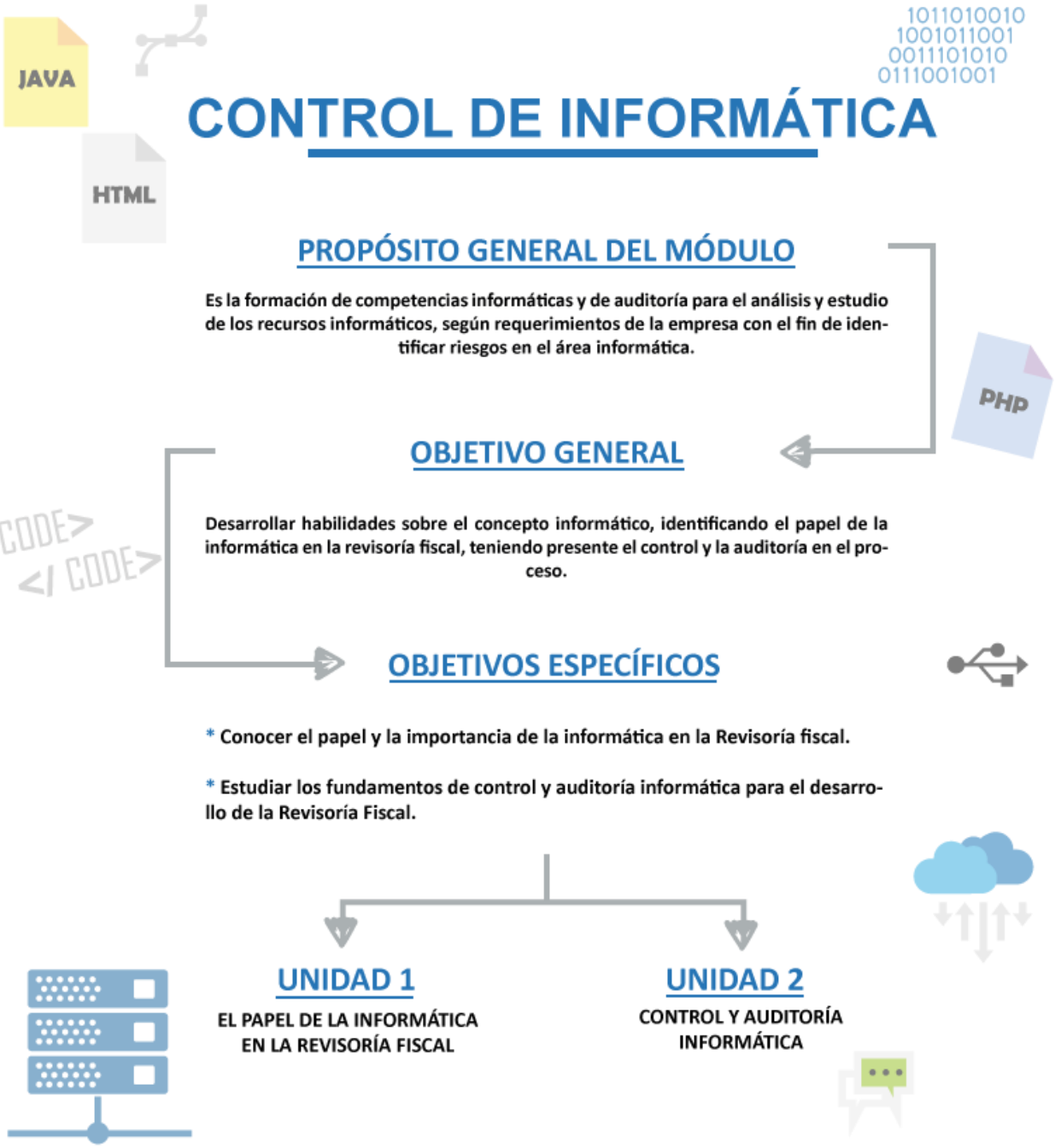
GRUPO DE APOYO

Personal de la Unidad CUR-Virtual
EDICIÓN Y MONTAJE
Primera versión. Febrero de 2011.
Segunda versión. Marzo de 2012
Tercera versión. noviembre de 2015
Cuarta versión. 2016

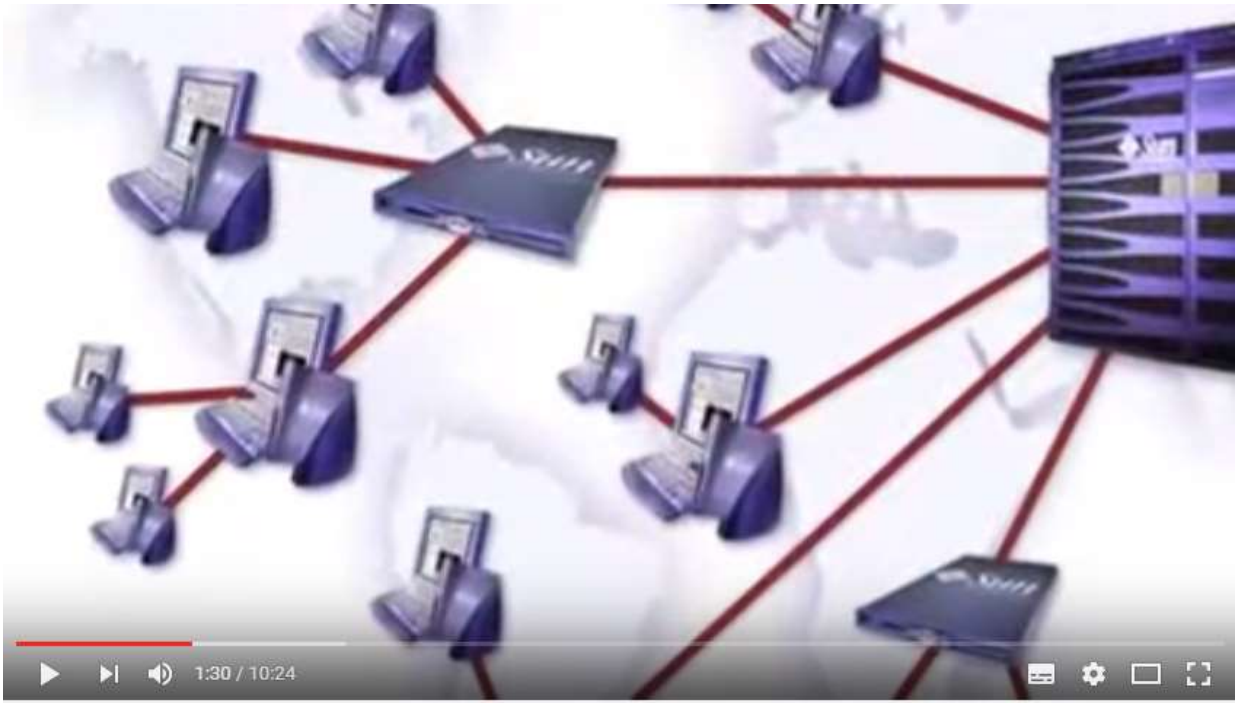
TABLA DE CONTENIDO

Pág.

1 MAPA DE LA ASIGNATURA

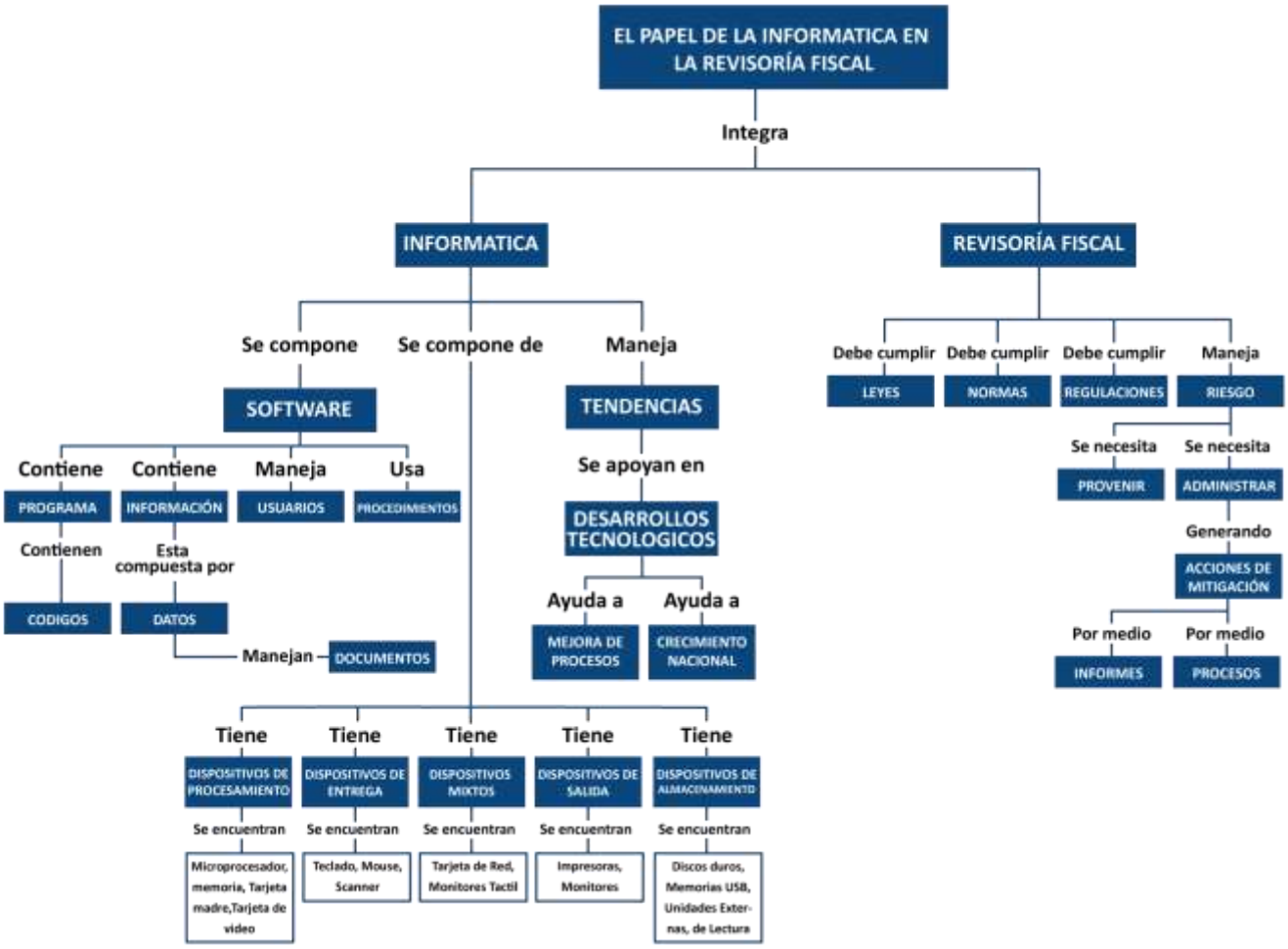


2 UNIDAD 1 EL PAPEL DE LA INFORMÁTICA EN LA REVISORÍA FISCAL



Legislación Informática: Enlace

2.1.1 RELACIÓN DE CONCEPTOS



OBJETIVO GENERAL

Conocer el papel y la importancia de la informática en la Revisoría fiscal.

OBJETIVOS ESPECÍFICOS

- Identificar la importancia de TI y la informática para la revisoría fiscal.
- Conocer las tendencias de la informática en el mundo de la tecnología.

2.2 TEMA 1 LA IMPORTANCIA DE TI Y LA INFORMÁTICA PARA EL REVISOR FISCAL.

Al llegar las TIC a la vida cotidiana, ya sea para su uso personal, social, académico y laboral, éstas han ido evolucionando progresivamente por la innovación de nuevas herramientas y plataformas, y en este proceso se encuentran las empresas para lograr el aprovechamiento de la tecnología en sus procesos.

Por ello, todos los profesionales, especialmente del área de la Revisoría Fiscal tienen la obligación de conocer y manejar estas herramientas tan innovadoras, para su buen uso en la mayoría de los procesos administrativos, contables y financieros, logrando un dominio que facilite y optimice el trabajo.

Este mundo cambia de manera acelerada y la continua capacitación de todos los profesionales es un modo de respuesta a las exigencias y demandas que esta sociedad les hará en un mercado laboral.

- Hardware
- Software
- Datos
- Procedimientos
- Usuarios
- Documentos

Enevis Rafael Reyes Moreno, 2013

Hardware

Hace referencia a la parte física de máquina considerada como el área tangible.

Componentes de hardware

El hardware está compuesto por cinco grupos de dispositivos:

Dispositivos de procesamiento

Es el elemento principal o centro neurálgico de una computadora y su misión consiste en coordinar y realizar todas las operaciones del sistema informático.

Ejemplo: board, procesador, memoria RAM, entre otros.

Dispositivos de entrada

También llamados periféricos o unidades de entrada, son los encargados de introducir los datos y los programas desde el exterior a la memoria principal para su utilización.

Ejemplo: teclado, ratón, lápiz óptico, la cámara de video, escáner, las pantallas sensibles al tacto entre otros.

Dispositivos de salida

Son aquellos dispositivos cuya misión es recoger y proporcionar al exterior los datos de salida o resultados de los procesos que realicen.

Ejemplo: monitor, impresoras y Plotter, entre otros.

Dispositivos de almacenamiento

También llamados de almacenamiento secundario o memoria auxiliar. Son los dispositivos de almacenamiento masivo de información que se utilizan para guardar datos y programas en el tiempo para su posterior utilización.

Ejemplo: discos duros, discos ópticos, cintas y discos de video digital.

Dispositivos mixtos

Son aquello que cumplen con la función de salida y entrada de información al sistema.

Ejemplo: la tarjeta de red, los modem, entre otros.

Enevis Rafael Reyes Moreno, 2013

DATOS

"El dato es una representación simbólica (numérica, alfabética, algorítmica, entre otras) de un atributo o característica de una entidad. Los datos describen hechos empíricos, sucesos y entidades.

Los datos aisladamente pueden no contener información humanamente relevante. Sólo cuando un conjunto de datos se examina conjuntamente a la luz de un enfoque, hipótesis o teoría se puede apreciar la información contenida en dichos datos. Los datos pueden consistir en números, estadísticas o proposiciones descriptivas. Los datos convenientemente agrupados, estructurados e interpretados se consideran que son la base de la información humanamente relevante que se pueden utilizar en la toma decisiones, la reducción de la incertidumbre o la realización de cálculos. Es de empleo muy común en el ámbito informático y, en general, prácticamente en cualquier investigación científica."

Consultado en http://es.wikipedia.org/wiki/Dato

PROCEDIMIENTOS

Un procedimiento es un conjunto de acciones u operaciones que tienen que realizarse de la misma forma, para obtener siempre el mismo resultado bajo las mismas circunstancias (por ejemplo, procedimiento de emergencia).

USUARIOS

En sentido general, un usuario es un conjunto de permisos y de recursos (o dispositivos) a los cuales se tiene acceso. Es decir, un usuario puede ser tanto una persona como una máquina o un programa, etc.

2.2.1 EJERCICIO DE APRENDIZAJE:

Nombre del ejercicio de aprendizaje:	Manejo de componentes
Identificar las características básicas de un equipo de cómputo, contemplando: procesador, memoria, disco de almacenamiento, dispositivos de entrada y salida. Deben solicitar una cotización de un equipo de cómputo física o en medio digital y hacer el estudio de cada característica .	
Solución del taller: Tercera generación del procesador Intel® Core™ i3-3220 (3MB Caché, 3.30 GHz) Windows 8 Pro, 64-bit, español 4 GB[1] SDRAM DDR3 a 1600 MHz Disco Duro SATA de 500GB 7200 RPM (3.0 Gb/s), 16MB Caché Gráficos integrados Intel® HD 1 año de ProSupport, con respuesta al siguiente día laborable	

PISTAS DE APRENDIZAJE

Recuerde que:
El recurso informático está compuesto por el hardware y el Software. Donde el software es la parte intangible y el hardware es lo tangible.

Tenga en cuenta:
El recurso informático es una herramienta estratégica para lograr mejores resultados en los procesos de la empresa.

Traiga a la memoria:
Que la evolución de los computadores inicia en:
1823: Charles Babbage. Máquina analítica
1939: John Atanasoff. ABC. Computador digital programable
1943: Alan Turing. Colossus. Computadora digital electrónica
1944: Howard Aiken. Mark 1. Calculadora automática
1946: ENIAC Máquina que calcula trayectoria
1951: UNIVAC 1
1952: Primer compilador
1956: aparecen los transistores
1964: BASIC Lenguaje de programación
1965: Intel Chip de Silicio
1971: surge el microprocesador
1973: Protocolo de internet
1975: Primer ordenador personal
Hoy: Portátiles i3, i5 y i7.

2.3 TEMA 2 TENDENCIAS DE LA INFORMÁTICA

IT Madrid ha identificado las principales tendencias tecnológicas que están modificando la informática tal y como la entendíamos hasta ahora. Tendencias clave que se están imponiendo en los entornos empresariales e impactando a gran velocidad en las organizaciones.

Marcan el desarrollo del sector tecnológico, la forma de trabajar en las organizaciones y lo hacen de manera rápida. Son las siete tendencias tecnológicas que, de acuerdo con IT Madrid, están "cambiando el rumbo de la informática".

Así, José Valentín Álvarez, decano y profesor de IT Madrid, la escuela de negocios especializada en TI, ha sido el encargado de realizar un análisis en el que detecta como principales tendencias tecnológicas hoy en día:

1. Green IT, que ha hecho que la industria desarrolle tecnologías más amables con el entorno, que promueven el uso de la energía de manera eficiente y emplean materiales biodegradables o menos contaminantes. Producto de ello, explican desde IT Madrid, ganan terreno las iniciativas de virtualización y optimización de los centros de datos.

https://billionphotos.com/Media/Detail/1651461/clipart-abstract-design-information-wireless-network

2. SaaS y Cloud Computing: software como servicio, que responde al acrónimo inglés SaaS y que evolucionó de ASP (Application Service Provider), es un modelo de implementación de software en las compañías, en el que la instalación, el mantenimiento, los respaldos y el soporte de las aplicaciones es responsabilidad del proveedor, al que se le paga por uso y que da acceso parametrizado y privado vía Internet a las empresas. Cloud computing. Este es un modelo que, ya no sólo el software, sino las capacidades tecnológicas flexibles y escalables proporciona a los clientes mediante tecnologías Web, con ventajas que ofrecen valor al negocio como movilidad, reducción de riesgos y costes, procesos de negocio prácticamente estandarizados, etc. Destaca en estas áreas el éxito de Salesforce.com, NetSuite, Intacct, Aplicor o Google Apps.

3. Gobierno IT: esta tendencia surge de la necesidad de alinear tecnología y negocio. Históricamente, los tecnólogos no conocen el negocio y los usuarios desconocen las actividades del departamento de sistemas. Para paliar este déficit en un momento en el que las inversiones en TI son relevantes, se han creado unidades

intermedias entre negocio e informática que racionalizan y justifican las inversiones, además de optimizar el uso de los recursos. Con las Oficinas de Proyectos, PMOs en sus siglas inglesas, emergen aplicaciones de Project Management, que ponen en orden y facilitan los proyectos informáticos, un ámbito en el que destacan proveedores como CA, Oracle o Microsoft.

4. Web 2.0: es una evolución en la forma de trabajar en la Web, cuya idea central es el proceso de colaboración y convergencia de muchas personas en un medio, lo que facilita la interrelación entre grupos tanto públicos como privados. Es Tim O'Reilly quien acuña este término, cuyas premisas son el fortalecimiento de las comunidades de usuarios y una gama especial de servicios. A partir de 2004, surgen herramientas y tecnologías o grupos de tecnologías que ayudan a su adopción como AJAX, Java Web, RSS/ATOM, SEM/SEO, blogs, JCC, Mashups, JSON, XML o APIs REST, entre otros.

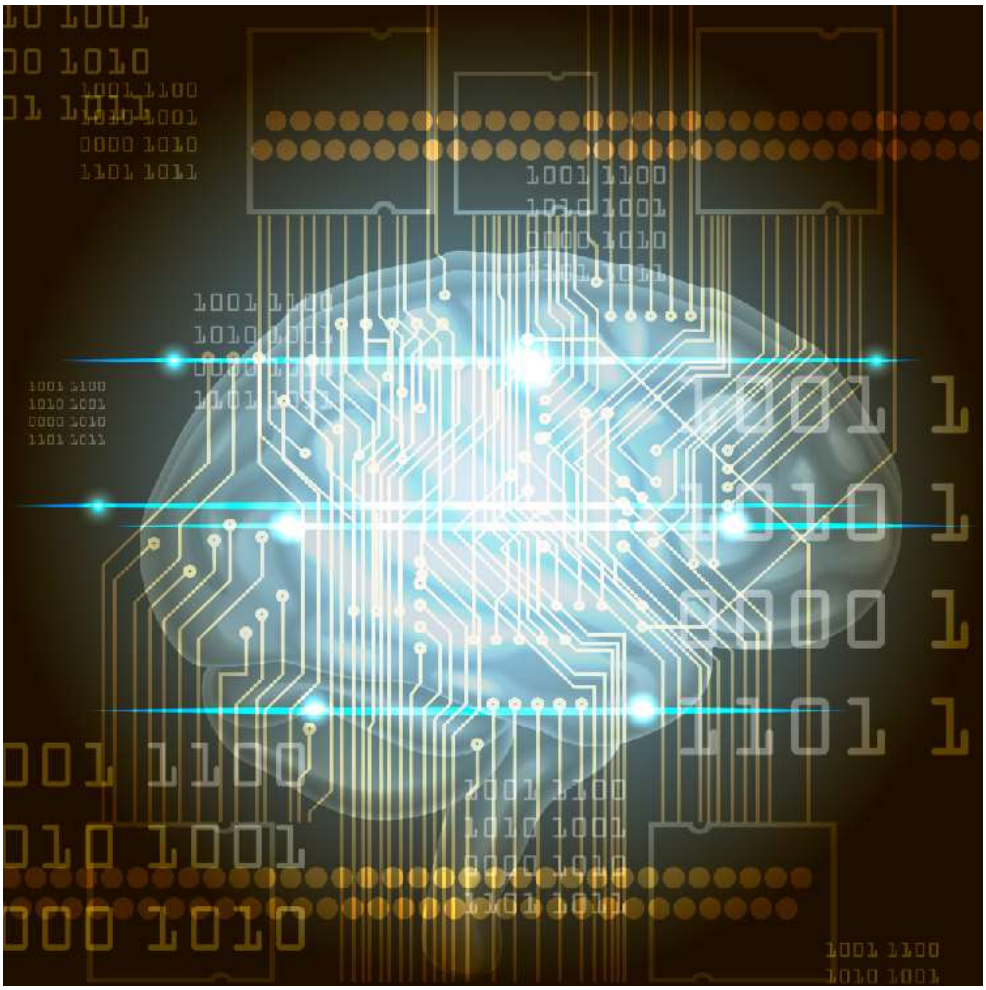
5. Tecnología móvil corporativa: la convergencia digital avanza y se consolidará como un referente tecnológico del siglo XXI. El Smartphone, además de telefonía, ofrece atributos similares a las de un PC, y se consigue una clara convergencia entre un teléfono móvil, un PC, una PDA y un dispositivo multimedia. Garantizar el acceso al correo corporativo, el ERP, el CRM, la intranet, LMS y otras aplicaciones corporativas será el objetivo de la próxima generación de aplicativos. Es un mercado en el que la competencia es fuerte, y la liberación de los sistemas operativos para Smartphone (Java, Windows Mobile, Symbian OS, Android, RIM BlackBerry, Linux, Mac o Palm OS).

6. Gestión del rendimiento: es una tecnología que, apoyada en el concepto de Business Intelligence, promueve el uso sistemático y organizado de los datos históricos de una empresa mediante la gestión de grandes volúmenes de datos y modernas técnicas estadísticas. Al gestionar el rendimiento, se pone en marcha una estrategia de control y seguimiento, a través de indicadores de gestión, de los objetivos y estrategias de la organización, de forma que se garantiza su cumplimiento y el ajuste de cualquier desviación de las metas establecidas. Es un concepto que se nutre de tecnologías robustas como gestores de bases de datos, herramientas de elevada capacidad analítica, etc. En esta área, destacan líderes como IBM, Oracle, SAP, Microsoft, Sun, etc.

7. Gestión de contenidos y/o gestión de activos digitales: la gestión de activos digitales (Digital Asset Management, DAM) es el proceso de identificar, clasificar, digitalizar, almacenar y recuperar datos e información no estructurada de todo tipo, con el fin de incrementar la productividad de las organizaciones que manejan grandes volúmenes de información: imágenes, vídeos, libros, documentos legales, mapas, etc. DAM ha irrumpido con fuerza gracias a la robustez de los sistemas de gestión de bases de datos, la potencia de las CPUs, la consolidación de XML como estándar y el aumento de las capacidades de almacenamiento. Destacan en este segmento de mercado IBM, EMC, Open Text, Oracle, Microsoft, Interwoven, Vignette, Hyland Software, Xerox o HP, entre otras.

Detectar y anteponerse a las tendencias que están moldeando la nueva generación de tecnología es clave para que las organizaciones puedan conseguir ventajas competitivas resulta especialmente urgente ya que, como explica José Valentín Álvarez, "el personal de TI debe comprender los cambios que se están produciendo en su

entorno para ampliar su visión, aportar valor añadido a su empresa y fortalecer el papel de las TI dentro de la compañía".

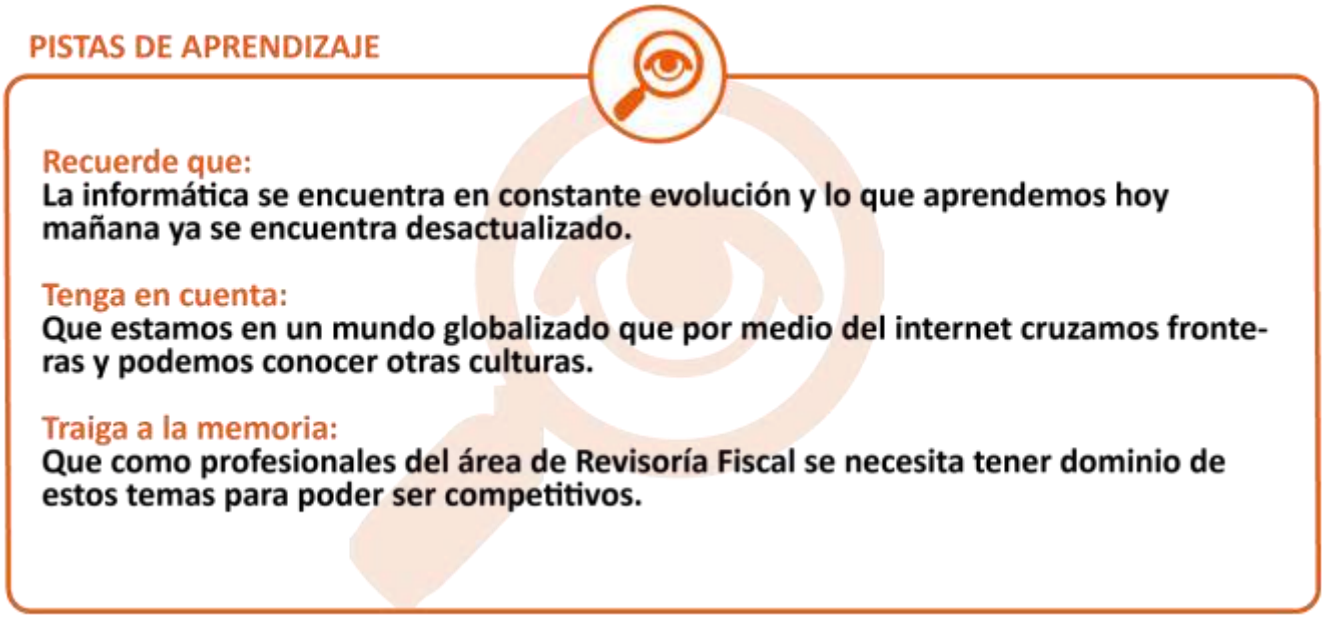


https://billionphotos.com/Media/Detail/1454606/clipart-Brain-Intelligence-Futuristic-Cyborg-Technology-vector

2.3.1 EJERCICIO DE APRENDIZAJE:

Nombre del ejercicio de aprendizaje:	Evaluación de tendencias, ENEVIS RAFAEL REYES MORENO

Realizar un ensayo sobre las tendencias y la evolución de los ambientes informáticos que se están viviendo en este momento.
Solución del taller: Ensayo por alumno:



2.3.2 TALLER DE ENTRENAMIENTO:

Nombre del taller:	Innovación tecnológica. Aplicación de la Web 2.0
Describa la actividad: entrar a la página de www.wikispaces.com y crear un wiki para consignar las asignaturas estudiadas en páginas independientes. Adicional a esto, construir una estructura con cada taller de entrenamiento.	

Actividad previa: descargar desde www.google.com un manual de wikispaces como herramientas colaborativas e iniciar el estudio de la plataforma del wiki.

Actividad:

Creación del wiki

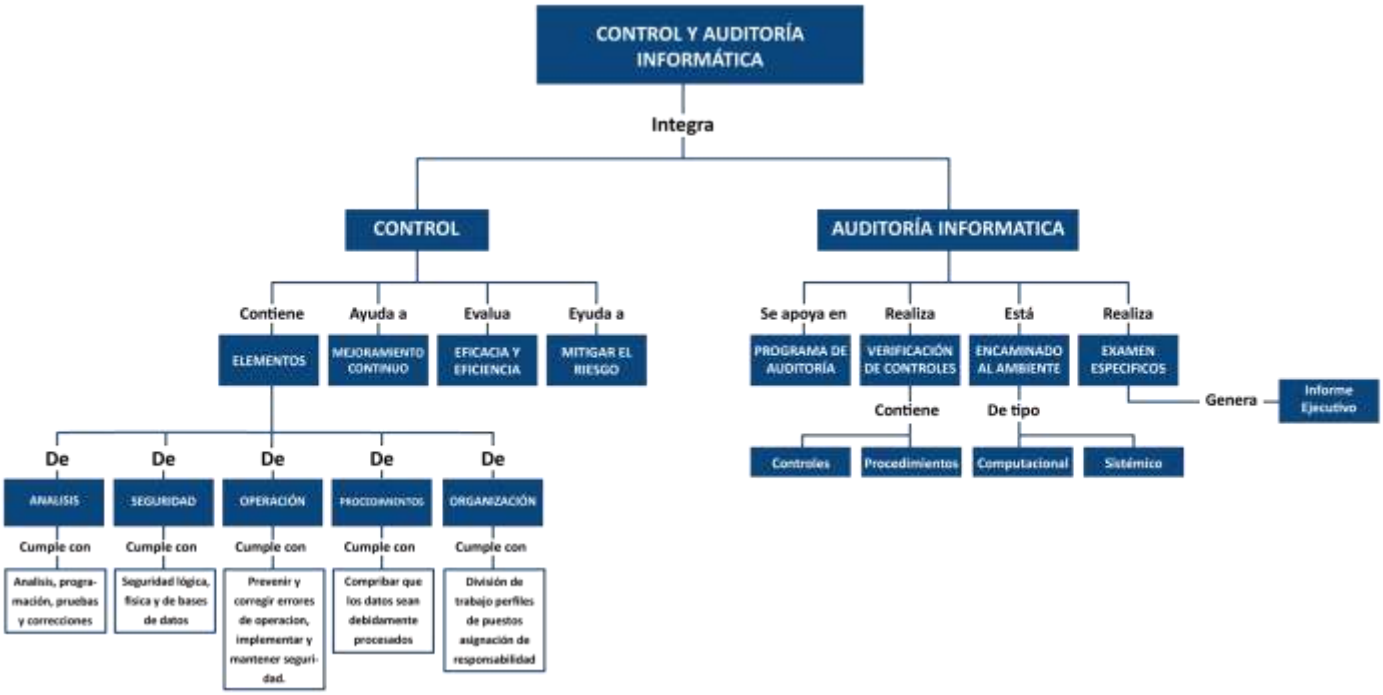
Configuración

Cargar archivos.

3 UNIDAD 2 CONTROL Y AUDITORÍA INFORMÁTICA

AUDITORIA INFORMATICA...wmv: Enlace

3.1.1 RELACIÓN DE CONCEPTOS



Enevis Rafael Reyes Moreno, 2013

OBJETIVO GENERAL

- Estudiar los fundamentos de control y auditoría informática para el desarrollo de la Revisoría Fiscal.

OBJETIVOS ESPECÍFICOS

- Conocer el proceso de auditoría informática para la ejecución de programas de auditoría.
- Ubicar al estudiante en la importancia del control y la revisoría fiscal.

3.2 TEMA 1 AUDITORÍA INFORMÁTICA

El concepto de auditoría informática según lo muestra Wikipedia es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. Permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes.

Los objetivos de la auditoría son identificar riesgos, evaluar y recomendar controles, que se convierte en una investigación crítica e independiente orientada al control de las actividades de una organización.

La auditoría en informática es la revisión y la evaluación de 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, con la finalidad de que a través del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoría en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y tengan un buen nivel de seguridad. Además, debe evaluar todo (informática, organización de centros de información, hardware y software).

PLANEACIÓN DE LA AUDITORÍA EN INFORMÁTICA

Para hacer una adecuada planeación de la auditoría en informática, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características de área dentro del organismo a auditar, sus sistemas, organización y equipo.

En el caso de la auditoría en informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de los dos objetivos:

- Evaluación de los sistemas y procedimientos.
- Evaluación de los equipos de cómputo.

Para hacer una planeación eficaz, lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, con base en esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

INVESTIGACIÓN PRELIMINAR

Se deberá observar el estado general del área, su situación dentro de la organización, si existe la información solicitada, si es o no necesaria y la fecha de su última actualización.

Se debe hacer la investigación preliminar solicitando y revisando la información de cada una de las áreas basándose en los siguientes puntos:

ADMINISTRACIÓN

Se recopila la información para obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitud de documentos para poder definir el objetivo y alcances del departamento.

PARA ANALIZAR Y DIMENSIONAR LA ESTRUCTURA POR AUDITAR SE DEBE SOLICITAR:

A NIVEL DEL ÁREA DE INFORMÁTICA

Objetivos a corto y largo plazo.

RECURSOS MATERIALES Y TÉCNICOS

Solicitar documentos sobre los equipos, número de ellos, localización y características.

- Estudios de viabilidad.
- Número de equipos, localización y las características (de los equipos instalados, por instalar y programados).
- Fechas de instalación de los equipos y planes de instalación.
- Contratos vigentes de compra, renta y servicio de mantenimiento.
- Contratos de seguros.
- Convenios que se tienen con otras instalaciones.

- Configuración de los equipos y capacidades actuales y máximas.
- Planes de expansión.
- Ubicación general de los equipos.
- Políticas de operación.
- Políticas de uso de los equipos.

SISTEMAS

Descripción general de los sistemas instalados y de los que estén por instalarse que contengan volúmenes de información.

- Manual de formas.
- Manual de procedimientos de los sistemas.
- Descripción genérica.
- Diagramas de entrada, archivos, salida.
- Salidas.
- Fecha de instalación de los sistemas.
- Proyecto de instalación de nuevos sistemas.

En el momento de hacer la planeación de la auditoría o bien su realización, debemos evaluar que pueden presentarse las siguientes situaciones.

Se solicita la información y se ve que:

- No tiene y se necesita.
- No se tiene y no se necesita.

Se tiene la información, pero:

- No se usa.
- Es incompleta.
- No está actualizada.
- No es la adecuada.
- Se usa, está actualizada, es la adecuada y está completa.

En el caso de que No se tenga y no se necesita, se debe evaluar la causa por la que no es necesaria. En el caso de que No se tenga, pero es necesaria, se debe recomendar que se elabore de acuerdo con las necesidades y con el uso que se le va a dar. En el caso de que se tenga la información pero no se utilice, se debe analizar por qué no se

usa. En caso de que se tenga la información, se debe analizar si se usa, si está actualizada, si es la adecuada y si está completa.

El éxito del análisis crítico depende de las consideraciones siguientes:

- Estudiar hechos y no opiniones (no se toman en cuenta los rumores ni la información sin fundamento).
- Investigar las causas, no los efectos.
- Atender razones, no excusas.
- No confiar en la memoria, preguntar constantemente.
- Criticar objetivamente y a fondo todos los informes y los datos recabados.

PERSONAL PARTICIPANTE

Una de las partes más importantes dentro de la planeación de la auditoría en informática es el personal que deberá participar y sus características.

Uno de los esquemas generalmente aceptados para tener un adecuado control es que el personal que intervengan esté debidamente capacitado, con alto sentido de moralidad, al cual se le exija la optimización de recursos (eficiencia) y se le retribuya o compense justamente por su trabajo.

Con estas bases se debe considerar las características de conocimientos, práctica profesional y capacitación que debe tener el personal que intervendrá en la auditoría. En primer lugar, se debe pensar que hay personal asignado por la organización, con el suficiente nivel para poder coordinar el desarrollo de la auditoría, proporcionar toda la información que se solicite y programar las reuniones y entrevistas requeridas.

Éste es un punto muy importante ya que, de no tener el apoyo de la alta dirección, ni contar con un grupo multidisciplinario en el cual estén presentes una o varias personas del área a auditar, sería casi imposible obtener información en el momento y con las características deseadas.

También se debe contar con personas asignadas por los usuarios para que en el momento que se solicite información o bien se efectúe alguna entrevista de comprobación de hipótesis, nos proporcionen aquello que se está solicitando, y complementen el grupo multidisciplinario, ya que se debe analizar no sólo el punto de vista de la dirección de informática, sino también el del usuario del sistema.

Para completar el grupo, como colaboradores directos en la realización de la auditoría se deben tener personas con las siguientes características:

- Técnico en informática.
- Experiencia en el área de informática.
- Experiencia en operación y análisis de sistemas.

- Conocimientos de los sistemas más importantes.

En caso de sistemas complejos se deberá contar con personal con conocimientos y experiencia en áreas específicas como base de datos, redes, etc. Lo anterior no significa que una sola persona tenga los conocimientos y experiencias señaladas, pero si deben intervenir una o varias personas con las características apuntadas.

Una vez que se ha hecho la planeación, se puede utilizar el formato señalado en el anexo 1, la figura, el organismo, las fases y subfases que comprenden la descripción de la actividad, el número de personas participantes, las fechas estimadas de inicio y terminación, el número de días hábiles y el número de días/hombre estimado. El control del avance de la auditoría lo podemos llevar mediante el anexo 2, el cual nos permite cumplir con los procedimientos de control y asegurarnos que el trabajo se está llevando a cabo de acuerdo con el programa de auditoría, con los recursos estimados y en el tiempo señalado en la planeación.

El hecho de contar con la información del avance nos permite revisar el trabajo elaborado por cualquiera de los asistentes. Como ejemplo de propuesta de auditoría en informática véase el anexo 3.

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:

- ¿Cuáles servicios se implementarán?
- ¿Cuándo se pondrán a disposición de los usuarios?
- ¿Qué características tendrán?
- ¿Cuántos recursos se requerirán?

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

- ¿Qué aplicaciones serán desarrolladas y cuándo?
- ¿Qué tipo de archivos se utilizarán y cuándo?
- ¿Qué bases de datos serán utilizadas y cuándo?
- ¿Qué lenguajes se utilizarán y en que software?

- ¿Qué tecnología será utilizada y cuando se implementará?
- ¿Cuántos recursos se requerirán aproximadamente?
- ¿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.

- ¿Qué estudios van a ser realizados al respecto?
- ¿Qué metodología se utilizará para dichos estudios?
- ¿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.

- ¿Contempla el plan estratégico las ventajas de la nueva tecnología?
- ¿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 con que 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:

- 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.
- Los requerimientos de los usuarios.
- 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:

- Planeada para ser desarrollada en el futuro.
- En desarrollo.
- En proceso, pero con modificaciones en desarrollo.
- En proceso con problemas detectados.
- En proceso sin problemas.
- 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:

- ¿Se está ejecutando en forma correcta y eficiente el proceso de información?
- ¿Puede ser simplificado para mejorar su aprovechamiento?
- ¿Se debe tener una mayor interacción con otros sistemas?
- ¿Se tiene propuesto un adecuado control y seguridad sobre el sistema?
- ¿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:

- Entradas.
- Salidas.
- Procesos.
- Especificaciones de datos.
- Especificaciones de proceso.
- Métodos de acceso.
- Operaciones.
- Manipulación de datos (antes y después del proceso electrónico de datos).
- Proceso lógico necesario para producir informes.
- Identificación de archivos, tamaño de los campos y registros.
- Proceso en línea o lote y su justificación.
- Frecuencia y volúmenes de operación.
- Sistemas de seguridad.
- Sistemas de control.
- Responsables.
- Número de usuarios.
- Dentro del estudio de los sistemas en uso se deberá solicitar:
- Manual del usuario.
- Descripción de flujo de información y/o procesos.
- Descripción y distribución de información.
- Manual de formas.
- Manual de reportes.
- Lista de archivos y especificaciones.
- Lo que se debe determinar en el sistema:
- En el procedimiento:
- ¿Quién hace, cuándo y cómo?
- ¿Qué formas se utilizan en el sistema?
- ¿Son necesarias, se usan, están duplicadas?
- ¿El número de copias es el adecuado?
- ¿Existen puntos de control o faltan?

En la gráfica de flujo de información:

- ¿Es fácil de usar?
- ¿Es lógica?
- ¿Se encontraron lagunas?
- ¿Hay faltas de control?

En el diseño:

- ¿Cómo se usará la herramienta de diseño si existe?
- ¿Qué tan bien se ajusta la herramienta al procedimiento?

EVALUACIÓN DEL DESARROLLO DEL SISTEMA

En esta etapa del sistema se deberán auditar los programas, su diseño, el lenguaje 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 tráfico 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:

- Dinámicos (susceptibles de modificarse).
- Estructurados (las interacciones de sus componentes o subsistemas deben actuar como un todo).
- Integrados (un solo objetivo). En él habrá sistemas que puedan ser interrelacionados y no programas aislados.
- Accesibles (que estén disponibles).
- Necesarios (que se pruebe su utilización).
- Comprensibles (que contengan todos los atributos).
- Oportunos (que esté la información en el momento que se requiere).

- Funcionales (que proporcionen la información adecuada a cada nivel).
- Estándar (que la información tenga la misma interpretación en los distintos niveles).
- Modulares (facilidad para ser expandidos o reducidos).
- Jerárquicos (por niveles funcionales).
- Seguros (que sólo las personas autorizadas tengan acceso).
- Únicos (que no duplique información).

NORMAS, TECNICAS Y PROCEDIMIENTOS DE AUDITORÍA INFORMÁTICA

El desarrollo de una auditoría se basa en la aplicación de normas, técnicas y procedimientos de auditoría. Para nuestro caso, estudiaremos aquellas enfocadas a la auditoría en informática.

Es fundamental mencionar que para el auditor en informática conocer los productos de

software que han sido creados para apoyar su función aparte de los componentes de la propia computadora resulta esencial, esto por razones económicas y para facilitar el manejo de la información.

El auditor desempeña sus labores mediante la aplicación de una serie de conocimientos especializados que vienen a formar el cuerpo técnico de su actividad. El auditor adquiere responsabilidades, no solamente con la persona que directamente contratan sus servicios, sin o con un número de personas desconocidas para él que van a utilizar el resultado de su trabajo como base para tomar decisiones.

La auditoría no es una actividad meramente mecánica, que implique la aplicación

de ciertos procedimientos cuyos resultados, una vez llevados a cabo son de

carácter indudable. La auditoría requiere el ejercicio de un juicio profesional, sólido,

maduro, para juzgar los procedimientos que deben seguirse y estimar los

resultados obtenidos.

NORMAS

Las normas de auditoría son los requisitos mínimos de calidad relativos a la personalidad del auditor, al trabajo que desempeña ya la información que rinde como resultado de este trabajo.

Las normas de auditoría se clasifican en:

a. Normas personales.

b. Normas de ejecución del trabajo.

c. Normas de información.

Normas personales

Son cualidades que el auditor debe tener para ejercer sin dolo una auditoría, basados en sus conocimientos profesionales, así como en un entrenamiento técnico, que le permita ser imparcial a la hora de dar sus sugerencias.

Normas de ejecución del trabajo

Son la planificación de los métodos y procedimientos, tanto como papeles de trabajo que el auditor aplicará dentro del proceso de auditoría.

Normas de información

Son el resultado que el auditor debe entregar a los interesados para que se den cuenta

de su trabajo, también es conocido como informe o dictamen.

Técnicas

Se define a las técnicas de auditoría como "los métodos prácticos de investigación y prueba que utiliza el auditor para obtener la evidencia necesaria que fundamente sus opiniones y conclusiones, su empleo se basa en su criterio o juicio, según las circunstancias".

Al aplicar su conocimiento y experiencia el auditor, podrá conocer los datos de la empresa u organización a ser auditada, que pudieran necesitar una mayor atención.

Las técnicas procedimientos están estrechamente relacionados, si las técnicas no son elegidas adecuadamente, la auditoría no alcanzará las normas aceptadas de ejecución, por lo cual las técnicas, así como los procedimientos de auditoría tienen una gran importancia para el auditor.

Según el IMCP en su libro *Normas y procedimientos de auditoría* las técnicas se clasifican

generalmente con base en la acción que se va a efectuar, estas acciones pueden ser oculares, verbales, por escrito, por revisión del contenido de documentos y por examen físico.

Siguiendo esta clasificación las técnicas de auditoría se agrupan específicamente de la

Siguiente manera:

- Estudio General
- Análisis
- Inspección
- Confirmación
- Investigación
- Declaración
- Certificación
- Observación
- Cálculo

Procedimientos

Al conjunto de técnicas de investigación aplicables a un grupo de hechos o circunstancias que nos sirven para fundamentar la opinión del auditor dentro de una auditoría, se les dan el nombre de procedimientos de auditoría en informática.

La combinación de dos o más procedimientos, derivan en programas de auditoría, y al conjunto de programas de auditoría se le denomina plan de auditoría, el cual servirá al auditor para llevar una estrategia y organización de la propia auditoría.

El auditor no puede obtener el conocimiento que necesita para sustentar su opinión en una sola prueba, es necesario examinar los hechos, mediante varias técnicas de aplicación simultánea.

En General los procedimientos de auditoría permiten:

- Obtener conocimientos del control interno.
- Analizar las características del control interno.
- Verificar los resultados de control interno.
- Fundamentar conclusiones de la auditoría.

Por esta razón el auditor deberá aplicar su experiencia y decidir cuál técnica o procedimiento de auditoría serán los más indicados para obtener su opinión.

Análisis de datos

Dentro de este trabajo, desarrollaremos diversos tipos de técnicas y procedimientos de auditoría, de los cuales destacan el análisis de datos, ya que para las organizaciones el conjunto de datos o información son de tal importancia que es necesario verificarlos y comprobarlos, así también tiene la misma importancia para el auditor ya que debe de utilizar diversas técnicas para el análisis de datos, las cuales se describen a continuación.

Comparación de programas

Esta técnica se emplea para efectuar una comparación de código (fuente, objeto o comandos de proceso) entre la versión de un programa en ejecución y la versión de un programa piloto que ha sido modificado en forma indebida, para encontrar diferencias.

Mapeo y rastreo de programas

Esta técnica emplea un software especializado que permite analizar los programas en ejecución, indicando el número de veces que cada línea de código es procesada y la de las variables de memoria que estuvieron presentes.

Análisis de código de programas

Se emplea para analizar los programas de una aplicación. El análisis puede efectuarse en forma manual (en cuyo caso sólo se podría analizar el código ejecutable).

Datos de prueba

Se emplea para verificar que los procedimientos de control incluidos los programas de una aplicación funcionen correctamente. Los datos de prueba consisten en la preparación de una serie de transacciones que contienen tanto datos correctos como datos erróneos predeterminados.

Datos de prueba integrados

Técnica muy similar a la anterior, con la diferencia de que en ésta se debe crear una entidad falsa dentro de los sistemas de información.

Análisis de bitácoras

Existen varios tipos de bitácoras que pueden ser analizadas por el auditor, ya sea en forma manual o por medio de programas especializados, tales como bitácoras de fallas del equipo, bitácoras de accesos no autorizados, bitácoras de uso de recursos, bitácoras de procesos ejecutados.

Simulación paralela

Técnica muy utilizada que consiste en desarrollar programas o módulos que simulen a los programas de un sistema en producción. El objetivo es procesar los dos programas o módulos de forma paralela e identificar diferencias entre los resultados de ambos.

ANÁLISIS DE BITÁCORAS

Hoy en día los sistemas de cómputo se encuentran expuestos a distintas amenazas, las

vulnerabilidades de los sistemas aumentan, al mismo tiempo que se hacen más complejos. El número de ataques también aumenta, por lo anterior, las organizaciones deben reconocer la importancia y utilidad de la información contenida en las bitácoras de los sistemas de cómputo, así como mostrar algunas herramientas que ayuden a automatizar el proceso de análisis de las mismas.

El crecimiento de Internet enfatiza esta problemática, los sistemas de cómputo generan una gran cantidad de información, conocidas como bitácoras o archivos logs, que pueden ser de gran ayuda ante un incidente de seguridad, así como para el auditor.

Una bitácora puede registrar mucha información acerca de eventos relacionados con el sistema que la genera los cuales pueden ser:

- Fecha y hora.
- Direcciones IP origen y destino.
- Dirección IP que genera la bitácora.
- Usuarios.
- Errores.

La importancia de las bitácoras es la de recuperar información ante incidentes de seguridad, detección de comportamiento inusual, información para resolver problemas, evidencia legal; es de gran ayuda en las tareas de cómputo forense.

Las Herramientas de análisis de bitácoras más conocidas son las siguientes:

- Para UNIX, Logcheck, SWATCH.
- Para Windows, LogAgent

Las bitácoras contienen información crítica, es por ello que deben ser analizadas, ya que están teniendo mucha relevancia, como evidencia en aspectos legales.

El uso de herramientas automatizadas es de mucha utilidad para el análisis de bitácoras, es importante registrar todas las bitácoras necesarias de todos los sistemas de cómputo para mantener un control de las mismas.

Técnicas de auditoría asistida por computadora

La utilización de equipos de computación en las organizaciones, ha tenido una repercusión importante en el trabajo del auditor, no sólo en lo que se refiere a los sistemas de información, sino también al uso de las computadoras en la auditoría.

Al llevar a cabo auditorías donde existen sistemas computarizados, el auditor se enfrenta a muchos problemas de muy diversa condición, uno de ellos, es la revisión de los procedimientos administrativos de control interno establecidos en la empresa que es auditada.

La utilización de paquetes de programas generalizados de auditoría ayuda en gran medida a la realización de pruebas de auditoría, a la elaboración de evidencias plasmadas en los papeles de trabajo.

Las técnicas de auditoría Asistidas por Computadora (CAAT) son la utilización de determinados paquetes de programas que actúan sobre los datos, llevando acabo con más frecuencia los siguientes trabajos:

- Selección e impresión de muestras de auditorías sobre bases estadísticas o no estadísticas, a lo que agregamos, sobre la base de los conocimientos adquiridos por los auditores.
- Verificación matemática de sumas, multiplicaciones y otros cálculos en los archivos del sistema auditado.
- Realización de funciones de revisión analítica, al establecer comparaciones, calcular razones, identificar fluctuaciones y llevar a cabo cálculos de regresión múltiple.
- Manipulación de la información al calcular subtotales, sumar y clasificar la información, volver a ordenar en serie la información, etc.
- Examen de registros de acuerdo con los criterios especificados.
- Búsqueda de alguna información en particular, la cual cumpla ciertos criterios, que se encuentra dentro de las bases de datos del sistema que se audita.

Consecuentemente, se hace indispensable el empleo de las CAAT que permiten al auditor, evaluar las múltiples aplicaciones específicas del sistema que emplea la unidad auditada, el examinar un diverso número de operaciones específicas del sistema, facilitar la búsqueda de evidencias, reducir al mínimo el riesgo de la auditoría para que los resultados expresen la realidad objetiva de las deficiencias, así como de las violaciones detectadas y elevar notablemente la eficiencia en el trabajo.

Teniendo en cuenta que se hacía imprescindible auditar sistemas informáticos; así como diseñar programas auditores, se deben incorporar especialistas informáticos, formando equipos multidisciplinarios capaces de incursionar en las auditorías informáticas y comerciales, independientemente de las contables, donde los

auditores que cumplen la función de jefes de equipo, están en la obligación de documentarse sobre todos los temas auditados.

De esta forma los auditores adquieren más conocimientos de los diferentes temas, pudiendo incluso, sin especialistas de las restantes materias realizar análisis de esos temas, aunque en ocasiones es necesario que el auditor se asesore con expertos, tales como, ingenieros industriales, abogados, especialistas de recursos humanos o de normalización del trabajo para obtener evidencia que le permita reunir elementos de juicio suficientes.

Evaluación del control interno

En un ambiente de evolución permanente, determinado por las actuales tendencias mundiales, las cuales se centran en el plano económico, soportadas por la evolución tecnológica, surge la necesidad de que la función de auditoría pretenda el mejoramiento de su gestión.

La práctica de nuevas técnicas para evaluar el control interno a través de las cuales, la función de auditoría informática pretende mejorar la efectividad de su función y con ello ofrecer servicios más eficientes y con un valor agregado.

La evolución de la teoría del control interno se definió con base en los principios de los controles como mecanismos o prácticas para prevenir, identificar actividades no autorizadas, Más tarde se incluyó el concepto de lograr que las cosas se hagan; la corriente actual define al control como cualquier esfuerzo que se realice para aumentar las posibilidades de que se logren los objetivos de la organización.

En este proceso evolutivo se considera actualmente, y en muchas organizaciones que el director de finanzas, contralor o al director de auditoría como los responsables principales del correcto diseño y adecuado funcionamiento de los controles internos.

Qué mejor prueba que la posibilidad de ponerlo en práctica si se pudiera obtener que el hecho de que la tecnología ya se ha probado y se encuentra en uso en todas partes, el benchmarking genérico requiere de una amplia conceptualización, pero con una

comprensión cuidadosa del proceso genérico.

3.2.1 EJERCICIO DE APRENDIZAJE:

Nombre del ejercicio de aprendizaje:	ENEVIS RAFAEL REYES MORENO Seguimiento a concepto sobre cargos y tipos de auditoría.

Realizar la investigación de los diferentes cargos generados en el proceso de auditoría Revisor Fiscal, Auditor Interno, Auditor Externo y Contralor. De igual forma, se debe investigar sobre los tipos de auditoría como: Auditoría Financiera, Auditoría Administrativa, Auditoría Operacional, Auditoría De Gestión, Auditoría De Cumplimiento, Auditoría De Control Interno, Auditoría Informática.
Solución del taller: Individual.

PISTAS DE APRENDIZAJE

Recuerde que:
Las empresas que tienen auditoría integral son aquellas que tienen su departamento de auditoría en las que aplican auditoría a todos los procesos.

Tenga en cuenta:
Los elementos de la auditoría implican, evidencias, pruebas, técnicas y procedimientos.

Traiga a la memoria:
Las etapas para realizar un trabajo de auditoría son Planeación, Ejecución e información.

3.3 TEMA 2 CONTROL Y REVISIÓN FISCAL

CONTROL DE PROYECTOS

Debido a las características propias del análisis y la programación, es frecuente que la implantación de los sistemas se retrase y 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 con 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.

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 más 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 al lugar 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 más las refacciones (este tipo de mantenimiento puede ser el adecuado para computadoras personales).

Al evaluar el mantenimiento se debe, primero, analizar cuál 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 cómputo?
Sí () NO ()

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

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

6. Solicite el plan de mantenimiento preventivo que debe ser proporcionado por el proveedor.
Sí ( ) NO ( )
¿Cuál?

7. ¿Cómo se notifican las fallas?

8. ¿Cómo se les da seguimiento?

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 y 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:

Aire acondicionado ()

Protección contra el fuego ()

(Señalar que tipo de protección)

Cerradura especial ()

Otra _____

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

3. ¿Qué 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?
Sí () NO ()

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

6. ¿Qué 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?
Sí () NO ()

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

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

10. ¿Qué medio se utiliza para almacenarlos?
Mueble con cerradura ( )
Bóveda ( )
Otro (especifique) _____

11. Este almacén está situado:
En el mismo edificio del departamento ( )
En otro lugar ( )
¿Cuál?_____

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

13. ¿Se certifica la destrucción o baja de los archivos defectuosos?
Sí () NO ()

14. ¿Se registran como parte del inventario las nuevas cintas que recibe la discoteca?
Sí () NO ()

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

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

17. ¿Qué 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?
Sí () NO ()

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

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

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

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

- Fecha de recepción ()
- Fecha en que se debe devolver ()
- Archivos que contiene ()
- Formatos ()
- Cifras de control ()
- Código de grabación ()
- Nombre del responsable que los presto ()
- 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?
Sí () NO ()

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

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

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

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

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

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

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

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

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

¿Con qué frecuencia?

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 cómputo?
Sí () NO ()

2. ¿Están actualizados los procedimientos?
Sí () 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 acción requerida ()
- 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)?
Sí () NO ()

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

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

8. ¿Existe un control que asegure la justificación de los procesos en el computador? (Que los procesos que se están autorizando y tengan una razón de ser procesados)
Sí ( ) 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?
Sí () 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 específicas 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 prohíbe a analistas y programadores la operación del sistema que programó o analizó?

19. ¿Se prohíbe 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? Sí () NO ()
- - ¿Se limitan los mensajes esenciales? Sí () NO ()
- Otras (especifique) _____

22. ¿Se tiene un control adecuado sobre los sistemas y programas que están en operación?
Sí ( ) 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?
Sí () NO ()

25. ¿Cuentan los operadores con una bitácora para mantener registros de cualquier evento y acción tomada por ellos?
Sí ( )
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?
Sí () 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?
SÍ () 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?
SÍ () NO ()

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

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

37. ¿Durante cuánto tiempo?

38. ¿Qué 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?
SÍ () NO ()

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

42. Indique qué 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?
Sí () NO ()

44. Indique como está organizado este archivo de bitácora.

Por fecha ()

Por fecha y hora ()

Por turno de operación ()

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?
Sí () NO ()

49. ¿Cómo se controlan los procesos en línea?

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

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

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

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?

- Usuario
- Analista
- Programadores
- Operadores
- Gerente de departamento
- Auditores internos
- Asesores
- 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:

- Estudio de la definición ()
- Discusión con el analista ()
- Diagrama de bloques ()

- Tabla de decisiones ()
- Prueba de escritorio ()
- Codificación ()
- ¿Es enviado a captura o los programadores capturan? ( )
- ¿Quién los captura? _____
- Compilación ()
- Elaborar datos de prueba ()
- Solicitar datos al analista ()
- Correr programas con datos ()
- Revisión de resultados ()
- Corrección del programa ()
- Documentar el programa ()
- Someter resultados de prueba ()
- 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.

CONTROL 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 pérdidas 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?
Sí () NO ()

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

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

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

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

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

SEGURIDAD LÓGICA Y CONFIDENCIAL

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional.

Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos. Ante esta situación, en el transcurso del siglo XX, el mundo ha sido testigo de la transformación de algunos aspectos de seguridad y de derecho.

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar el llamado ""virus" de las computadoras, el cual, aunque tiene diferentes intenciones se encuentra principalmente para paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco.

Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus.

El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Dichos paquetes han sido populares desde hace muchos años en el mundo de las computadoras grandes, y los principales proveedores ponen a disposición de clientes algunos de estos paquetes.

El sistema integral de seguridad debe comprender:

- Elementos administrativos.
- Definición de una política de seguridad.
- Organización y división de responsabilidades.
- Seguridad física y contra catástrofes (incendio, terremotos, etc.).
- Prácticas de seguridad del personal.
- Elementos técnicos y procedimientos.
- Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.
- Aplicación de los sistemas de seguridad, incluyendo datos y archivos.
- El papel de los auditores, tanto internos como externos.
- Planeación de programas de desastre y su prueba.

Se debe evaluar el nivel de riesgo que puede tener la información para poder hacer un adecuado estudio costo/beneficio entre el costo por pérdida de información y el costo de un sistema de seguridad, para lo cual se debe considerar lo siguiente:

- Clasificar la instalación en términos de riesgo (alto, mediano, pequeño).
- Identificar aquellas aplicaciones que tengan un alto riesgo.
- Cuantificar el impacto en el caso de suspensión del servicio en aquellas aplicaciones con un alto riesgo.
- Formular las medidas de seguridad necesarias dependiendo del nivel de seguridad que se requiera.
- La justificación del costo de implantar las medidas de seguridad para poder clasificar el riesgo e identificar las aplicaciones de alto riesgo, se debe preguntar lo siguiente:
  - ¿Qué sucedería si no se puede usar el sistema?
  - Si la contestación es que no se podría seguir trabajando, esto nos sitúa en un sistema de alto riego.

La siguiente pregunta es:

- ¿Qué implicaciones tiene el que no se obtenga el sistema y cuánto tiempo podríamos estar sin utilizarlo?
- ¿Existe un procedimiento alterno y que problemas nos ocasionaría?
- ¿Qué se ha hecho para un caso de emergencia?

Una vez que se ha definido, el grado de riesgo, hay que elaborar una lista de los sistemas con las medias preventivas que se deben tomar, así como las correctivas en caso de desastre señalándole a cada uno su prioridad.

Hay que tener mucho cuidado con la información que sale de la oficina, su utilización y que sea borrada al momento de dejar la instalación que está dando respaldo.

Para clasificar la instalación en términos de riesgo se debe:

- Clasificar los datos, información y programas que contienen información confidencial que tenga un alto valor dentro del mercado de competencia de una organización, e información que sea de difícil recuperación.
- Identificar aquella información que tenga un gran costo financiero en caso de pérdida o bien puede provocar un gran impacto en la toma de decisiones.
- Determinar la información que tenga una gran pérdida en la organización y, consecuentemente, puedan provocar hasta la posibilidad de que no pueda sobrevivir sin esa información.

Para cuantificar el riesgo es necesario que se efectúen entrevistas con los altos niveles administrativos que sean directamente afectados por la suspensión en el procesamiento y que cuantifiquen el impacto que les puede causar este tipo de situaciones.

Para evaluar las medidas de seguridad se debe:

- Especificar la aplicación, los programas y archivos.

- Las medidas en caso de desastre, pérdida total, abuso y los planes necesarios.
- Las prioridades que se deben tomar en cuanto a las acciones a corto y largo plazo.
- En cuanto a la división del trabajo se debe evaluar que se tomen las siguientes precauciones, las cuales dependerán del riesgo que tenga la información y del tipo y tamaño de la organización.
- El personal que prepara la información no debe tener acceso a la operación.
- Los análisis y programadores no deben tener acceso al área de operaciones y viceversa.
- El operador no debe tener acceso ir restringido a las librerías ni a los lugares donde se tengan los archivos almacenados; es importante separar las funciones de librería y de operación.
- Los operadores no deben ser los únicos que tengan el control sobre los trabajos procesados y no deben hacer las correcciones a los errores detectados.

Al implantar sistemas de seguridad puede, reducirse la flexibilidad en el trabajo, pero no debe reducir la eficiencia.

SEGURIDAD FÍSICA

El objetivo es establecer políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de datos, información debido a contingencias como incendio, inundaciones, huelgas, disturbios, sabotaje, etc. y continuar en medio de emergencia hasta que sea restaurado el servicio completo.

Entre las precauciones que se deben revisar están:

- Los ductos del aire acondicionado deben estar limpios, ya que son una de las principales causas del polvo y se habrá de contar con detectores de humo que indiquen la posible presencia de fuego.
- En las instalaciones de alto riesgo se debe tener equipo de fuente no interrumpible, tanto en la computadora como en la red y los equipos de teleproceso.
- En cuanto a los extintores, se debe revisar en número de estos, su capacidad, fácil acceso, peso y tipo de producto que utilizan. Es muy frecuente que se tengan los extintores, pero puede suceder que no se encuentren recargados o bien que sean de difícil acceso de un peso tal que sea difícil utilizarlos.
- Esto es común en lugares donde se encuentran trabajando hombres y mujeres y los extintores están a tal altura o con un peso tan grande que una mujer no puede utilizarlos.
- Otro de los problemas es la utilización de extintores inadecuados que pueden provocar mayor perjuicio a las máquinas (extintores líquidos) o que producen gases tóxicos.
- También se debe ver si el personal sabe usar los equipos contra incendio y si ha habido prácticas en cuanto a su uso.
- Se debe verificar que existan suficientes salidas de emergencia y que estén debidamente controladas para evitar robos por medio de estas salidas.

- Los materiales más peligrosos son las cintas magnéticas que al quemarse, producen gases tóxicos y el papel carbón que es altamente inflamable.

Tomando en cuenta lo anterior se elaboró el siguiente cuestionario:

1. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información?
Sí () NO ()

2. ¿Existen una persona responsable de la seguridad?
Sí () NO ()

3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?
Sí () NO ()

4. ¿Existe personal de vigilancia en la institución?
SÍ () NO ()

5. ¿La vigilancia se contrata?
a) Directamente ( )
b) Por medio de empresas que venden ese servicio ( )

6. ¿Existe una clara definición de funciones entre los puestos clave?
SÍ () NO ()

7. ¿Se investiga a los vigilantes cuando son contratados directamente?
SÍ () NO ()

8. ¿Se controla el trabajo fuera de horario?
SÍ () NO ()

9. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?
SÍ () NO ()

10. ¿Existe vigilancia en el departamento de cómputo las 24 horas?
SÍ () NO ()

11. ¿Existe vigilancia a la entrada del departamento de cómputo las 24 horas?
a) Vigilante ( )

b) Recepcionista ( )
c) Tarjeta de control de acceso ( )
d) Nadie ( )

12. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?
SÍ () NO ()

13. ¿Se ha instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?
SÍ () NO ()

14. El edificio donde se encuentra la computadora está situado a salvo de:
a) Inundación ( )
b) Terremoto ( )
c) Fuego ( )
d) Sabotaje ( )

15. ¿El centro de cómputo tiene salida al exterior?
SÍ () NO ()

16. Describa brevemente la construcción del centro de cómputo, de preferencia proporcionando planos y material con que está construido y equipo (muebles, sillas etc.) dentro del centro.

17. ¿Existe control en el acceso a este cuarto?
a) Por identificación personal ( )
b) Por tarjeta magnética ( )
c) por claves verbales ( )
d) Otras ( )

18. ¿Son controladas las visitas y demostraciones en el centro de cómputo?
Sí () NO ()

19. ¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática?
Sí () NO ()

20. ¿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?
Sí () NO ()

21. Existe alarma para:

a) Detectar fuego (calor o humo) en forma automática ( )
b) Avisar en forma manual la presencia del fuego ( )
c) Detectar una fuga de agua ( )
d) Detectar magnéticos ( )
e) No existe ( )

22. ¿Dónde están estas alarmas?

a) En el departamento de cómputo ( )
b) En la cintoteca y discoteca ( )

23. ¿Existe alarma para detectar condiciones anormales del ambiente?

a) En el departamento de cómputo ( )
b) En la cintoteca y discoteca ( )
c) En otros lugares ( )

24. ¿La alarma es perfectamente audible?

SÍ () NO ()

25. Esta alarma también está conectada

a) Al puesto de guardias ( )
b) A la estación de Bomberos ( )
c) A ningún otro lado ( )

Otro_____

26. ¿Existen extintores de fuego?

a) Manuales ( )
b) Automáticos ( )
c) No existen ( )

27. ¿Se ha instruido el personal en el manejo de los extintores?

SÍ () NO ()

28. ¿Los extintores, manuales o automáticos a base de (TIPO SÍ NO)

a) Agua ( ) ( )
b) Gas ( ) ( )
c) Otros ( ) ( )

29. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?

SÍ () NO ( )

30. Si es que existen extintores automáticos, ¿son activado por detectores automáticos de fuego?
SÍ () NO ()

31. Si los extintores automáticos son a base de agua, ¿se han tomado medidas para evitar que el agua cause más daño que el fuego?
Sí () NO ()

32. Si los extintores automáticos son a base de gas, ¿se han tomado medidas para evitar que el gas cause más daño que el fuego?
Sí () NO ()

33. Existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos para que el personal
a) Corte la acción de los extintores por tratarse de falsas alarmas Sí ( ) NO ( )
b) Pueda cortar la energía Eléctrica Sí ( ) NO ( )
c) Pueda abandonar el local sin peligro de intoxicación Sí ( ) NO ( )
d) Es inmediata su acción Sí ( ) NO ( )

34. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?
Sí () NO ()

35. ¿Saben que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionada por fuego?
Sí () NO ()

36. ¿El personal ajeno a operación sabe qué hacer en el caso de una emergencia (incendio)?
Sí () NO ()

37. ¿Existe salida de emergencia?
Sí () NO ()

38. Esta puerta solo es posible abrirla:
a) Desde el interior ( )
b) Desde el exterior ( )
c) Ambos Lados ( )

39. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?
Sí () NO ()

40. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?
Sí () NO ()

41. Se han tomado medidas para minimizar la posibilidad de fuego:
a) Evitando artículos inflamables en el departamento de cómputo ( )
b) Prohibiendo fumar a los operadores en el interior ( )
c) Vigilando y manteniendo el sistema eléctrico ( )
d) No se ha previsto ( )

42. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?
Sí () NO ()

43. ¿Se limpia con frecuencia el polvo acumulado debajo del piso falso si existe?
Sí () NO ()

44. ¿Se controla el acceso y préstamo en la
a) Discoteca? ( )
b) Cintoteca? ( )
c) Programoteca? ( )

45. Explique la forma como se ha clasificado la información vital, esencial, no esencial etc.

46. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?
SI () NO ()

47. Explique la forma en que están protegidas físicamente estas copias (bóveda, cajas de seguridad etc.) que garantice su integridad en caso de incendio, inundación, terremotos, etc.

48. ¿Se tienen establecidos procedimientos de actualización a estas copias?
Sí () NO ()

49. Indique el número de copias que se mantienen, de acuerdo con la forma en que se clasifique la información:
0 1 2 3

50. ¿Existe departamento de auditoría interna en la institución?
Sí () NO ()

51. ¿Este departamento de auditoría interna conoce todos los aspectos de los sistemas?
SÍ () NO ()

52. ¿Qué tipos de controles ha propuesto?

53. ¿Se cumplen?
SÍ () NO ()

54. ¿Se auditan los sistemas en operación?
SÍ () NO ()

55. ¿Con que frecuencia?
a) Cada seis meses ( )
b) Cada año ( )
c) Otra (especifique) ( )

56. ¿Cuándo se efectúan modificaciones a los programas, a iniciativa de quién es?
a) Usuario ( )
b) Director de informática ( )
c) Jefe de análisis y programación ( )
d) Programador ( )
e) Otras (especifique) _____

57. La solicitud de modificaciones a los programas se hacen en forma
a) Oral ( )
b) Escrita ( )
En caso de ser escrita solicite formatos.

58. Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?
SÍ () NO ()

59. ¿Existe control estricto en las modificaciones?
SÍ () NO ()

60. ¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?
SÍ () NO ()

61. Si se tienen terminales conectadas, ¿se ha establecido procedimientos de operación?
SÍ () NO ()

62. Se verifica identificación:
a) De la terminal ( )
b) Del Usuario ( )
c) No se pide identificación ( )

63. ¿Se ha establecido qué información puede ser ingresada y por qué persona?
Sí () NO ()

64. ¿Se ha establecido un número máximo de violaciones en sucesión para que la computadora cierre esa terminal y se dé aviso al responsable de ella?
Sí () NO ()

65. ¿Se registra cada violación a los procedimientos con el fin de llevar estadísticas y frenar las tendencias mayores?
SÍ () NO ()

66. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones? Y ¿Cuáles son?

- () Recepción de documentos_____
- () Información Confidencial_____
- () Captación de documentos_____
- () Cómputo Electrónico_____
- () Programas_____
- () Discotecas y Cinto tecas_____
- () Documentos de Salida_____
- () Archivos Magnéticos_____
- () Operación del equipo de computación_____
- () En cuanto al acceso de personal_____
- () Identificación del personal_____
- () Policia_____
- () Seguros contra robo e incendio_____
- () Cajas de seguridad_____
- () Otras (especifique)_____

SEGURIDAD EN LA UTILIZACIÓN DEL EQUIPO

En la actualidad los programas y los equipos son altamente sofisticados y sólo algunas personas dentro del centro de cómputo conocen en detalle el diseño, lo que puede provocar que puedan producir algún deterioro a los sistemas si no se toman las siguientes medidas:

1) Se debe restringir el acceso a los programas y a los archivos.

2) Los operadores deben trabajar con poca supervisión y sin la participación de los programadores, y no deben modificar los programas ni los archivos.

3) Se debe asegurar en todo momento que los datos y archivos usados sean los adecuados, procurando no usar respaldos inadecuados.
4) No debe permitirse la entrada a la red a personas no autorizadas, ni a usar las terminales.
5) Se debe realizar periódicamente una verificación física del uso de terminales y de los reportes obtenidos.
6) Se debe monitorear periódicamente el uso que se le está dando a las terminales.
7) Se debe hacer auditorías periódicas sobre el área de operación y la utilización de las terminales.
8) El usuario es el responsable de los datos, por lo que debe asegurarse que los datos recolectados sean procesados completamente. Esto sólo se logrará por medio de los controles adecuados, los cuales deben ser definidos desde el momento del diseño general del sistema.
9) Deben existir registros que reflejen la transformación entre las diferentes funciones de un sistema.
10) Debe controlarse la distribución de las salidas (reportes, cintas, etc.).
11) Se debe guardar copias de los archivos y programas en lugares ajenos al centro de cómputo y en las instalaciones de alta seguridad; por ejemplo: los bancos.
12) Se debe tener un estricto control sobre el acceso físico a los archivos.
13) En el caso de programas, se debe asignar a cada uno de ellos una clave que identifique el sistema, subsistema, programa y versión.

También evitará que el programador ponga nombres que nos signifiquen nada y que sean difíciles de identificar, lo que evitará que el programador utilice la computadora para trabajos personales. Otro de los puntos en los que hay que tener seguridad es en el manejo de información. Para controlar este tipo de información se debe:

1) Cuidar que no se obtengan fotocopias de información confidencial sin la debida autorización.
2) Sólo el personal autorizado debe tener acceso a la información confidencial.
3) Controlar los listados tanto de los procesos correctos como aquellos procesos con terminación incorrecta.
4) Controlar el número de copias y la destrucción de la información y del papel carbón de los reportes muy confidenciales.

El factor más importante de la eliminación de riesgos en la programación es que todos los programas y archivos estén debidamente documentados.

El siguiente factor en importancia es contar con los respaldos, y duplicados de los sistemas, programas, archivos y documentación necesarios para que pueda funcionar el plan de emergencia.

- -Equipo, programas y archivos.
- -Control de aplicaciones por terminal.
- -Definir una estrategia de seguridad de la red y de respaldos.
- -Requerimientos físicos.
- -Estándar de archivos.
- -Auditoría interna en el momento del diseño del sistema, su implantación y puntos de verificación y control.

SEGURIDAD AL RESTAURAR EL EQUIPO

En un mundo que depende cada día más de los servicios proporcionados por las computadoras, es vital definir procedimientos en caso de una posible falta o siniestro. Cuando ocurra una contingencia, es esencial que se conozca en detalle el motivo que la originó y el daño causado, lo que permitirá recuperar en el menor tiempo posible el proceso perdido. También se debe analizar el impacto futuro en el funcionamiento de la organización y prevenir cualquier implicación negativa.

En todas las actividades relacionadas con las ciencias de la computación, existe un riesgo aceptable, y es necesario analizar y entender estos factores para establecer los procedimientos que permitan analizarlos al máximo y en caso que ocurran, poder reparar el daño y reanudar la operación lo más rápidamente posible.

En una situación ideal, se deberían elaborar planes para manejar cualquier contingencia que se presente.

Analizando cada aplicación se deben definir planes de recuperación y reanudación, para asegurarse que los usuarios se vean afectados lo menos posible en caso de falla o siniestro. Las acciones de recuperación disponibles a nivel operativo pueden ser algunas de las siguientes:

En algunos casos es conveniente no realizar ninguna acción y reanudar el proceso.

Mediante copias periódicas de los archivos se puede reanudar un proceso a partir de una fecha determinada.

El procesamiento anterior complementado con un registro de las transacciones que afectaron a los archivos permitirá retroceder en los movimientos realizados a un archivo al punto de tener la seguridad del contenido del mismo a partir de él reanudar el proceso.

Analizar el flujo de datos y procedimientos y cambiar el proceso normal por un proceso alterno de emergencia.

Reconfigurar los recursos disponibles, tanto de equipo y sistemas como de comunicaciones.

Cualquier procedimiento que se determine que es el adecuado para un caso de emergencia deberá ser planeado y probado previamente.

Este grupo de emergencia deberá tener un conocimiento de los posibles procedimientos que puede utilizar, además de un conocimiento de las características de las aplicaciones, tanto desde el punto técnico como de su prioridad, el nivel de servicio planeado y su influjo en la operación de la organización.

Además de los procedimientos de recuperación y reinicio de la información, se deben contemplar los procedimientos operativos de los recursos físicos como hardware y comunicaciones, planeando la utilización de equipos que permitan seguir operando en caso de falta de la corriente eléctrica, caminos alternos de comunicación y utilización de instalaciones de cómputo similares. Estas y otras medidas de recuperación y reinicio deberán ser planeadas y probadas previamente como en el caso de la información.

El objetivo del siguiente cuestionario es evaluar los procedimientos de restauración y repetición de procesos en el sistema de cómputo.

1) ¿Existen procedimientos relativos a la restauración y repetición de procesos en el sistema de cómputo?
Sí () NO ()

2) Enuncie los procedimientos mencionados en el inciso anterior

3) ¿Cuentan los operadores con alguna documentación en donde se guarden las instrucciones actualizadas para el manejo de restauraciones?
Sí () NO ()

En el momento que se hacen cambios o correcciones a los programas y/o archivos se deben tener las siguientes precauciones:

1) Las correcciones de programas deben ser debidamente autorizadas y probadas. Con esto se busca evitar que se cambien por nueva versión que antes no ha sido perfectamente probada y actualizada.

2) Los nuevos sistemas deben estar adecuadamente documentos y probados.

3) Los errores corregidos deben estar adecuadamente documentados y las correcciones autorizadas y verificadas.

Los archivos de nuevos registros o correcciones ya existentes deben estar documentados y verificados antes de obtener reportes.

PROCEDIMIENTOS DE RESPALDO EN CASO DE DESASTRE

Se debe establecer en cada dirección de informática un plan de emergencia el cual ha de ser aprobado por la dirección de informática y contener tanto procedimiento como información para ayudar a la recuperación de interrupciones en la operación del sistema de cómputo.

El sistema debe ser probado y utilizado en condiciones anormales, para que, en caso de usarse en situaciones de emergencia, se tenga la seguridad que funcionará.

La prueba del plan de emergencia debe hacerse sobre la base de que la emergencia existe y se han de utilizar respaldos.

Se deben evitar suposiciones que, en un momento de emergencia, hagan inoperante el respaldo, en efecto, aunque el equipo de cómputo sea aparentemente el mismo, puede haber diferencias en la configuración, el sistema operativo, en disco etc.

El plan de emergencia una vez aprobado, se distribuye entre personal responsable de su operación, por precaución es conveniente tener una copia fuera de la dirección de informática.

En virtud de la información que contiene el plan de emergencia, se considerará como confidencial o de acceso restringido.

La elaboración del plan y de los componentes puede hacerse en forma independiente de acuerdo con los requerimientos de emergencia, La estructura del plan debe ser tal que facilite su actualización.

Para la preparación del plan se seleccionará el personal que realice las actividades claves del plan. El grupo de recuperación en caso de emergencia debe estar integrado por personal de administración de la dirección de informática, debe tener tareas específicas como la operación del equipo de respaldo, la interfaz administrativa.

Los desastres que pueden suceder podemos clasificar así:

a) Completa destrucción del centro de cómputo,
b) Destrucción parcial del centro de cómputo,
c) Destrucción o mal funcionamiento de los equipos auxiliares del centro de cómputo (electricidad, aire, acondicionado, etc.)

d) Destrucción parcial o total de los equipos descentralizados,
e) Pérdida total o parcial de información, manuales o documentación,
f) Pérdida de la personal clave, y
g) Huelga o problemas laborales.

El plan en caso de desastre debe incluir:

- La documentación de programación y de operación.
- Los equipos:
  - El equipo completo.
  - El ambiente de los equipos.
- Datos y archivos.
- Papelería y equipo accesorio.
- Sistemas (sistemas operativos, bases de datos, programas).

El plan en caso de desastre debe considerar todos los puntos por separado y en forma integral como sistema. La documentación estará en todo momento tan actualizada como sea posible, ya que en muchas ocasiones no se tienen actualizadas las últimas modificaciones y eso provoca que el plan de emergencia no pueda ser utilizado.

Cuando el plan sea requerido debido a una emergencia, el grupo deberá:

- Asegurarse de que todos los miembros sean notificados,
- Informar al director de informática,
- Cuantificar el daño o pérdida del equipo, archivos y documentos para definir qué parte del plan debe ser activada.
- Determinar el estado de todos los sistemas en proceso,
- Notificar a los proveedores del equipo cual fue el daño.

Establecer la estrategia para llevar a cabo las operaciones de emergencias tomando en cuenta:

- Elaboración de una lista con los métodos disponibles para realizar la recuperación.
- Señalamiento de la posibilidad de alternar los procedimientos de operación (por ejemplo, cambios en los dispositivos, sustituciones de procesos en línea por procesos en lote).
- Señalamiento de las necesidades para armar y transportar al lugar de respaldo todos los archivos, programas, etc., que se requieren.
- Estimación de las necesidades de tiempo de las computadoras para un periodo largo.

Cuando ocurra la emergencia, se deberá reducir la carga de procesos, analizando alternativas como:

- Posponer las aplicaciones de prioridad más baja.
- Cambiar la frecuencia del proceso de trabajos.
- Suspender las aplicaciones en desarrollo.

Por otro lado, se debe establecer una coordinación estrecha con el personal de seguridad a fin de proteger la información.

Respecto a la configuración del equipo hay que tener toda la información correspondiente al hardware y software del equipo propio y del respaldo.

Deberán tenerse todas las especificaciones de los servicios auxiliares tales como energía eléctrica, aire acondicionado, etc., a fin de contar con servicios de respaldo adecuados y reducir al mínimo las restricciones de procesos, se deberán tomar en cuenta las siguientes consideraciones:

- Mínimo de memoria principal requerida y el equipo periférico que permita procesar las aplicaciones esenciales.
- Se debe tener documentados los cambios de software.

En caso de respaldo en otras instituciones, previamente se deberá conocer el tiempo de computadora disponible.

Es conveniente incluir en el acuerdo de soporte recíproco los siguientes puntos:

- Configuración de equipos.
- Configuración de equipos de captación de datos.
- Sistemas operativos.
- Configuración de equipos periféricos.

3.3.1 EJERCICIO DE APRENDIZAJE:

Nombre del ejercicio de aprendizaje:	**ENEVIS RAFAEL REYES MORENO:** Generando Cuestionario

¿Qué cuestionario se podría realizar para validar el proceso en el campo de proyectos (CONTROL DE PROYECTOS)?

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 qué 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? Enuméralos 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.

Ejemplo de documento remisorio:

Medellín, xx de xxx de 200x
Señores
CIA XYZ S.A.
Atención Doctor Pepito Pérez
Gerente General
Asunto: informe sobre revisión de claves de acceso

Se han revisado la asignación y manejo de las claves de acceso de los diferentes funcionarios de la entidad, este trabajo se realizó entre los días xx a xx de este mes. Sobre el mismo se encontraron situaciones Irregulares que se enuncian en la Planilla de Auditoría adjunta, así mismo se formulan una serie de recomendaciones que ayudan a mejorar o corregir los errores al igual se identifican los beneficios que estas medidas traerían para la entidad.

Atentamente,
XXXXX XXXXXXXX XXXXX
Auditora General

Ejemplo de planilla de auditoría:

Cia XYZ S.A.
Departamento de Auditoría Interna
Informe sobre revisión de las claves de acceso

HALLAZGOS	RECOMENDACIONES	BENEFICIOS
1. El Departamento de Sistemas asigna mensualmente una clave de acceso para ser utilizada por los funcionarios del departamento de Contabilidad	1.1. Las claves de acceso las debe definir cada uno de los usuarios de las aplicaciones. 1.2. En el Departamento de Sistemas sólo se deben asignar las claves iniciales para cada uno de los empleados de la empresa 1.3. Las claves de acceso se deben cambiar frecuentemente, pero no en forma periódica, teniendo como tiempo máximo 30 días de utilización de una clave.	➢ Con el propósito de garantizar que las claves sean personales e intransferibles. ➢ Si varias personas trabajan con una misma clave, no se pueden asignar responsabilidades. ➢ Si cada una de las dependencias de la empresa cumple con su labor, su trabajo sería desarrollado con eficiencia, eficacia y efectividad. ➢ Con el cambio frecuente de claves se protege la empresa de fraudes informáticos
2. xxxxxxxx xxxxxxxxxx xxxxx xxxxxxx	2.1. xxxxxxxxxx xxxxxx xx xxxx xxxxx 2.2. xxxxxxxxxx xxxxxx xxxx xx xxxxx xxxxxx	➢ xxxxxxx xxxxxxxx xxxxxxxx xx xxxxx xxxxxxxxxx xxxxxxxxx xxx
3. xxxx xxxx xxxxx xxx xx xx xxx xxxx.	3.1. xxxx xxx xxx xxxxxx xx xxxx xx xxx	➢ xxxxxxx xxxxxxxx xxxxxxxx xx xxxxx xxxx. ➢ xxxxxxx xxxxxxxxx xxx ➢ xx xxxxxxxx xxxxxxxxxx xxx xxxxxxxxxxxxxxxxx xxxx.

MARGARITA MARÍA VÁSQUEZ MONTOYA
Auditora General

Medellín, xx de xxxx de 200x

3.3.2 TALLER DE ENTRENAMIENTO:

Nombre del ejercicio de aprendizaje:	Elaboración de un programa de auditoría
Realizar un programa de auditoría informática para una institución educativa teniendo presente los siguientes puntos: 1. **Componente a auditar** 2. **Objetivos: general y específicos** 3. **Alcance** 4. **Metodología** 5. **Normas: legales y administrativas**	

6. **Procedimientos**
7. **Áreas o cargos con lo que se hace contacto**
8. **Personal participante de auditoría**
9. **Duración**
10. **Horario**
11. **Recursos**

Se debe terminar con la simulación de la ejecución y desarrollo de documentos remisorios y planilla de auditoría.

Respuesta ANAXO 1.

PISTAS DE APRENDIZAJE

Recuerde que:
Los objetivos de la auditoría son identificar riesgos y evaluar y recomendar controles, que se convierte en una investigación crítica e independiente orientada al control de las actividades de una organización.

Tenga en cuenta:
Que los alcances en un programa de auditoría deben ser definidos en un nivel de detalle que evite malos entendidos con el cliente.

Traiga a la memoria:
Un proceso de auditoría sin informes de auditoría no tiene sentido. Y no cumple con el objetivo de la auditoría.

4 PISTAS DE APRENDIZAJE

Recuerde que:

El recurso informático está compuesto por el hardware y el Software. Donde el software es la parte intangible y el hardware es lo tangible.

Tenga en cuenta:

El recurso informático es una herramienta estratégica para lograr mejores resultados en los procesos de la empresa.

Traiga a la memoria:

Que la evolución de los computadores inicia en:

1823: Charles Babbage. Máquina analítica.

1939: John Atanasoff. ABC. Computador digital programable.

1943: Alan Turing. Colossus. Computadora digital electrónica.

1944: Howard Aiken. Mark 1. Calculadora automática.

1946: ENIAC Máquina que calcula trayectoria.

1951: UNIVAC 1.

1952: Primer compilador.

1956: aparecen los transistores.

1964: BASIC Lenguaje de programación.

1965: Intel Chip de Silicio.

1971: surge el microprocesador.

1973: Protocolo de internet.

1975: Primer ordenador personal-

Hoy: Portátiles i3, i5 y i7.

Recuerde que:

La Informática se encuentra en constante evolución y lo que aprendemos hoy mañana ya se encuentra desactualizado.

Tenga en cuenta:

Que estamos en un mundo globalizado que por medio del internet cruzamos fronteras y podemos conocer otras culturas.

Traiga a la memoria:

Que como profesionales del área de Revisoría Fiscal se necesita tener dominio de estos temas para poder ser competitivos.

Recuerde que:

Las empresas que tienen auditoría integral son aquellas que tienen su departamento de auditoría en las que aplican auditoría a todos los procesos.

Tenga en cuenta:

Los elementos de la auditoría implican, evidencias, pruebas, técnicas y procedimientos.

Traiga a la memoria:

Que las etapas para realizar un trabajo de auditoría son Planeación, Ejecución e información.

Recuerde que:

Los objetivos de la auditoría son identificar riesgos y evaluar y recomendar controles, que se convierte en una investigación crítica e independiente orientada al control de las actividades de una organización.

Tenga en cuenta:

Que los alcances en un programa de auditoría deben ser definidos en un nivel de detalle que evite malos entendidos con el cliente.

Traiga a la memoria:

Un proceso de auditoría sin informes de auditoría no tiene sentido. Y no cumple con el objetivo de la auditoría.

5 GLOSARIO

Sistema de información: es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

Conjunto de datos: un "Conjunto de datos" o "dataset" es una colección de datos normalmente tabulada. Por cada elemento (o individuo) se indican varias características.

Hipótesis científica: es una proposición aceptable que ha sido formulada a través de la recolección de información y datos, aunque no esté confirmada, sirve para responder de forma alternativa a un problema con base científica.

Informática: conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores.

Investigación científica: la investigación es una actividad humana orientada a la obtención de nuevos conocimientos y su aplicación para la solución a problemas o interrogantes de carácter científico.

Software: es equipamiento lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

Procedimientos: es una secuencia de pasos repetible y determinista; es decir, una en que siempre se irán obteniendo los mismos conjuntos de valores de salida, para los mismos conjuntos de valores de entrada.

Programas: un programa informático es un conjunto de instrucciones que una vez ejecutadas realizarán una o varias tareas en una computadora. Sin programas, estas máquinas no pueden funcionar. Al conjunto general de programas, se le denomina software.

Información: es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Usuario: en sentido general, un usuario es un conjunto de permisos y de recursos (o dispositivos) a los cuales se tiene acceso. Es decir, un usuario puede ser tanto una persona como una máquina, un programa, etc.

Códigos: el código binario, código fundamental en el que se basan los ordenadores, el más simple pues solo consta de dos elementos (0) y (1) que combinados de distintas maneras como impulsos eléctricos ponen las bases para la informática.

Datos: el dato es una representación simbólica (numérica, alfabética, algorítmica, entre otros) de un atributo o característica de una entidad. Los datos describen hechos empíricos, sucesos y entidades.

Documentos: es un testimonio material de un hecho o acto realizado en el ejercicio de sus funciones por instituciones o personas físicas, jurídicas, públicas o privadas, registrado en una unidad de información en cualquier tipo de soporte (papel, cintas, discos magnéticos, fotografías, etc.)

Hardware: se refiere a todas las partes tangibles de un sistema informático. Sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos. Son cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado

Dispositivos de procesamiento. Encargado del procesamiento de los datos, ejemplo: board, procesador, memoria RAM, entre otros.

Dispositivos de entrada. Generan entrada de datos al sistema, ejemplo: teclado, ratón, lápiz óptico, la cámara de video, escáner, las pantallas sensibles al tacto.

Dispositivos de salida. Permiten la salida de datos del sistema, ejemplo: monitor, impresoras y Plotter.

Dispositivos de almacenamiento. Realizan la función de almacenar los datos, ejemplo: discos duros, discos ópticos, cintas y discos de video digital.

Dispositivos mixtos: tienen la cualidad de permitir la entrada y salida de información y datos del sistema, ejemplo: la tarjeta de red, los modem, entre otros.

Revisoría fiscal: es una institución que es ejercida en cabeza de un profesional de la Contaduría, capaz de dar Fe Pública sobre la razonabilidad de los estados financieros, validar informes con destino a las entidades gubernamentales y juzgar sobre los actos de los administradores.

Leyes: son normas jurídicas dictadas por el legislador, es decir, un precepto establecido por la autoridad competente

Regulaciones: acción y efecto de regular, Proceso mediante el cual se mantiene constante una magnitud o condición, reglamentación determinación de las reglas que gobiernan algo.

Normas: es una regla u ordenación del comportamiento dictada por una autoridad competente, cuyo incumplimiento trae aparejado una sanción.

Riesgo: es la vulnerabilidad de "bienes jurídicos protegidos" ante un posible o potencial perjuicio o daño para las personas y cosas, particularmente, para el medio ambiente.

Prevenir: prever, conocer de antemano un daño o perjuicio y tomar las medidas necesarias.

Administrar: es la ciencia social y técnica encargada de la planificación, organización, dirección y control de los recursos (humanos, financieros, materiales, tecnológicos, del conocimiento, etc.) de una organización, con el fin de obtener el máximo beneficio posible; este beneficio puede ser económico o social, dependiendo de los fines perseguidos por la organización.

Mitigación: es la reducción de la vulnerabilidad, es decir la atenuación de los daños potenciales sobre la vida y los bienes causados por un evento.

Informes: el informe es un documento escrito en prosa informativa (científica, técnica, o comercial) con el propósito de comunicar información a un nivel más alto en una organización.

Procesos: un proceso es un conjunto de actividades o eventos (coordinados u organizados) que se realizan o suceden (alternativa o simultáneamente) bajo ciertas circunstancias con un fin determinado.

Control: se refiere al sistema u oficina que se encarga de verificar que ocurra lo que debería ocurrir.

Control interno o de gestión: es un conjunto de áreas funcionales en una empresa y de acciones especializadas en la comunicación y control al interior de la empresa.

Mejoramiento continuo: James Harrington (1993). Para él mejorar un proceso significa cambiarlo para hacerlo más efectivo, eficiente y adaptable, qué cambiar y cómo cambiar depende del enfoque específico del empresario y del proceso.

Elementos: cada una de las partes que forman un sistema.

Análisis: en sentido amplio, es la descomposición de un todo en partes para poder estudiar su estructura, sistemas operativos, funciones etc.

Seguridad: proviene de la palabra seguritas del latín, cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien.

Operación: combinación de números y operadores o de expresiones matemáticas a las que se aplica a unas reglas para obtener un resultado.

Organización: corresponde al proceso de organización de los talentos (humanos, financieros y materiales) de los que dispone la empresa, para alcanzar los objetivos deseados.

División de trabajo: es la especialización y cooperación de las fuerzas laborales en diferentes tareas y roles, con el objetivo de mejorar la eficiencia.

Perfiles de puestos

Auditoría informática: la auditoría informática es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas.

Programa de auditoría: son una serie de pasos que permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos.

Sistémico: la Sistémica puede ser considerada un nuevo nombre para todas las investigaciones relacionadas con la Teoría de Sistemas y la ciencia de sistemas.

6 BIBLIOGRAFÍA

Solís M, G. (2002): "Reingeniería de la Auditoría Informática". Trillas. México.

Díaz, Miguel. (2005): "Guía para la implementación del Sistema de Gestión de Seguridad de la Información ISO 17799". MANAGEMENT SYSTEMS

Sánchez, W. (2006): "Control interno conceptual y práctico". Investigar Editores. Segunda Edición.

PRIATTINI Mario G., Emilio del Peso: 1999, Auditoría Informática, un enfoque práctico. Editorial Ra-MA...

COHEN, Daniel. Sistemas de Información para los Negocios, un enfoque de toma de Decisiones. McGraw Hill.

DAVIS, Gordon. Sistemas de información Gerencial. McGraw Hill.

GIL, Ignacio. Sistemas y Tecnologías de la información para la Gestión. McGraw Hill.

McLEOD, Raymond. Sistemas de información Gerencial

Jorge Rene Quiñonez Folgar, Procedimientos y técnicas de auditoría. http://www.gerencie.com/procedimientos-y-tecnicas-de-auditoria.html

6.1 FUENTES DIGITALES O ELECTRÓNICAS

http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica

http://www.monografias.com

http://es.wikipedia.org/wiki/Dato

http://www.techweek.es/gestion-ti/informes/1005337003501/tendencias-tecnologicas-cambiando-informatica.1.html

http://www.slideshare.net/josar2/presentacion-tendencias-2011-jorge-callalle

http://ciberconta.unizar.es/LECCION/seguro/100.HTM

www.isaca.org

http://biblioteca.remington.edu.co/es/