**La información es el principal activo de la empresa**

Para la información se exigen requerimientos de:

* Calidad
* Controles
* Seguridad
* Economicidad

**Por ello**

* Las gerencias deben establecer sistemas de control interno que soporten en forma adecuada los procesos críticos del negocio.
* Las organizaciones exitosas entienden y administran los riesgos asociados de la implementación de tecnologías de información.

***Todo lo anterior justifica la necesidad de contar con una herramienta de control como lo es la auditoria informática.***

**El concepto de auditoria**

Consiste en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple con las condiciones que le gan sido prescritas.

**Concepto de consultoría**

La consultoría consiste en dar asesoramiento o consejo sobre lo que se ha de hacer, o como llevar a cabo adecuadamente una determinada actividad para obtener los fines deseados.

**Definición de auditoria en informática**

Para determinar si un sistema de información o proceso informático salvaguarda los activos empresariales informáticos, mantiene la integridad de los datos y lleva a cabo eficazmente los fines de la organización, utilizando eficientemente los recursos.

**Activos informáticos**

* Información
* Hardware
* Software
* Personas

**Objetivos de la auditoria informática**

* Control de la función informática
* La operatividad
* Seguridad
* Identificación de las áreas de mejoras
* Atenuación de los riesgos(controles)
* El análisis de la eficiencia y eficacia de los sistemas informáticos
* La verificación del cumplimiento de la normativa
* La revisión de la gestión de los recursos informáticos
* Protección de los activos e integridad de datos

**Aportes de la auditoria a las organizaciones**

* Eficiencia
* Eficacia
* Calidad
* Rentabilidad
* Seguridad
* Operatividad
* Estandarización

**Tipos de auditorías informáticas**

**Auditoria interna**

La auditoria interna es la realizada con rcursos materiales y personal que pertenece a la organización auditada.

**Auditoria externa**

Es la realizada por empresas y personas afines a la organización a auditar, es siempre remunerada, y se le presupone una mayor objetividad que a la auditoria interna, debido al mayor distanciamiento que hay entre auditores y auditados.

**Razones para una auditoria externa**

* Necesidad de auditar una materia de gran especialización, para lo cual los auditores propios no están suficientemente capacitados
* Contrastar algún informa interno con el que resulte de uno externo
* Servir como mecanismo protector de posibles auditorias informáticas externos

**La función de auditoria**

La función auditora debe ser absolutamente independiente; no tiene carácter ejecutivo, ni son vinculantes sus conclusiones y queda a cargo de la organización tomar las decisiones pertinentes

La auditoría contiene elementos de análisis, de verificación y exposición de debilidades y disfunciones. Aunque pueden aparecer sugerencias para eliminar las debilidades antedichas, estas sugerencias son plasmadas en el informe final de la auditoria que recibe el nombre de recomendaciones.

**Causas que justifican auditorias informáticas desde la visión de un jefe de informatica**

**Síntomas de descoordinación y desorganización**

Cuando no coinciden los objetivos de la informática con los de la organización (no hay alineamiento).

Cuando ocurre algún cambio masivo de personal.

**Síntomas de inseguridad**

**Evaluación de nivel de riesgos**

* Seguridad lógica
* Seguridad física
* Confidencialidad
* Continuidad de servicio
* Centro de proceso de datos fuera de control

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

**Síntomas de debilidades económico-financiero**

Cuando ocurre un incremento desmesurado de los costos como necesidad de justificar inversiones de informáticas.

Desviaciones presupuestarias significativas.

Costos y plazos de nuevos proyectos deben auditarse simultáneamente con el desarrollo del proyecto y al órgano que realizo la petición.

**La deontología**

Se relaciona con la ética y la moral, para observar la concepción humanista, y poder satisfacer al mundo externo, tiene que ver con creencias.

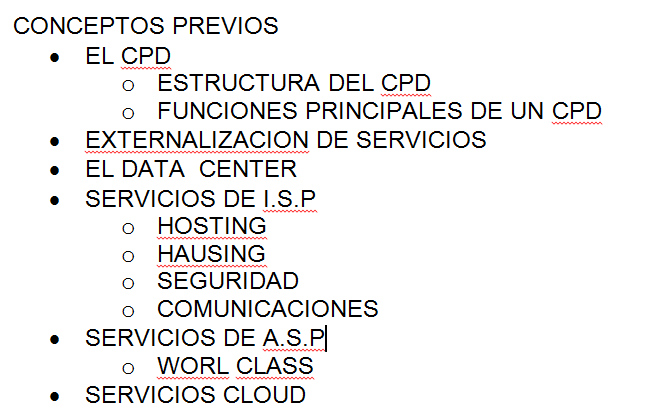
**Principales principios deontológicos**

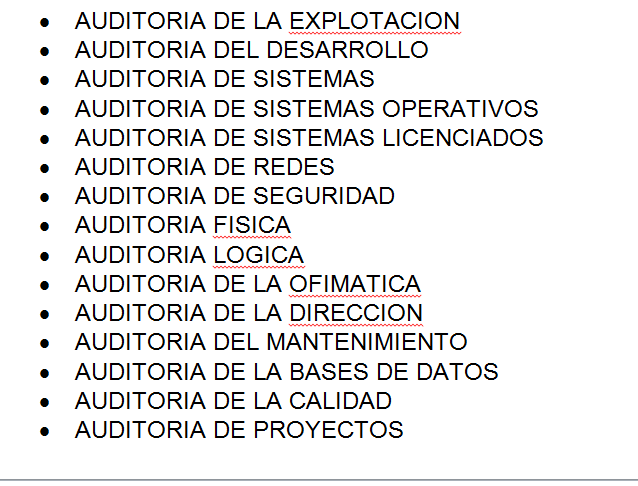
* Principio de independencia
* Principio de información suficiente
* Principio de integridad moral
* Principio de legalidad
* Principio de libre competencia
* Principio de no discriminación
* Principio de no injerencia
* Principio de precisión
* Principio de publicidad adecuada
* Principio de responsabilidad
* Principio de secreto profesional

**El código de ética de ISACA**

Requieren que los miembros cumplan con normas de conducta.

**Áreas de auditoria informática**

****

****

**Papeles de trabajo**

Es el legajo (carpeta que contiene todas las evidencias y documentos de formato) que emite el auditor.

**Procedimientos**

Es el conjunto de pasos necesarios para desarrollar una actividad determinada, los cuales deben estar debidamente documentados.

**Procedimientos administrativos**

Son documentos que describen la implementación del procedimiento diagramas

**Criterios de auditoria**

Es el conjunto de políticas y normas empleadas en la emisión de una opinión

**Conclusiones de la auditoria**

Resultado de una auditoria que proporciona el equipo auditor tras considerar los objetivos de la auditoria, las evidencias.

**Alcance de la auditoria**

Define la extensión y los límites de la auditoria.

**Evidencia de la auditoria**

Es cualquier información usada por el auditor de si para determinar si la entidad o los datos que están siendo auditados cumplen con los criterios u objetivos de auditoria establecidos.

**Determinantes para evaluar la calidad de las evidencias**

* Independencia del proveedor de la evidencia
* Calificación de la persona que suministra la información
* Objetividad de la evidencia

**Muestreo**

* Muestreo estadístico
* Muestreo no estadístico que se realiza a juicio del auditor

**Hallazgo de la auditoria**

Las evidencias que son evaluadas frente a criterios de auditoria y que son respaldadas y probadas.

**Las conformidades**

La conformidad debe resumirse para indicar las funciones, y procesos que se han auditado los hallazgos individuales de conformidad y su evidencia.

**Las no conformidades**

Están deben ser registradas y calificadas de acuerdo a su gravedad. **Deben ser revisadas con el auditado para obtener el reconocimiento.**

**Opinión con reserva**

Cualquier limitación que impida la aplicación de los dispuesto por una norma técnica.

**Directrices o políticas**

Son documentos de alto nivel que representan la filosofía corporativa de una organización deben ser claras y precisas.

**Normas**

Son estándares que definen criterios obligatorios que deben cumplirse.

**Seguridad informática**

Es un proceso y no un producto que abarca la información tanto en medios físicos como electrónicos, independiente si ellos involucran personas y tecnologías o relaciones con socios del negocio, cliente o terceros.

**La información**

la información es un bien que como otros tiene valor para una organización y consecuentemente necesita ser protegida en forma apropiada (justificación de la auditoria).

**La seguridad de la información**

La seguridad de la información la protege de una amplia gama de amenazas con el fin de asegurar la continuidad del negocio, minimizar el daño y maximizar el retorno de la inversión y oportunidades del negocio.

Se caracteriza por:

* La confidencialidad: consiste en asegurar que la información sea accesible solo para y por aquellos usuarios autorizados para tener acceso.
  + Es el costo de L compromiso
  + Solo tiene acceso a los activos aquellos que están autorizados
* La integridad: consiste en salvaguardar que la información y los métodos de procesamiento sean exactos y completos.
  + Integridad no es lo mismo que exactitud
  + Integridad es lo que debe estar correcto y debe ser confiable
  + Se puede tener integridad sin exactitud, pero no exactitud sin integridad
* La disponibilidad: consiste en asegurar que los usuarios autorizados tengan acceso a la información y bienes asociados cuando lo requieran. Comprende:
  + Servidores y estaciones de trabajo
  + Sitios web
  + Aplicaciones criticas

La seguridad de la información se logra mediante la implementación de un adecuado conjunto de controles, tales como:

* Políticas
* Practicas
* Normas
* Procedimientos
* Estructura organizacional informática
* Funciones de software
* Capacitación

Un gobierno efectivo de seguridad de la información debe lograr:

* Alinear la seguridad de información con la estrategia de negocio
* Ejecutar medidas para mitigar riesgos
* Optimizar las inversiones en seguridad
* Medir, monitorear e informar