

## I.S.A.C.A

### *Information System Audit Control Association*

Asociación mundial con título omernacional: 'CISA'

En Bruselas están pensando que para ser Auditor sea necesaria la posesión de este título.

Todo lo que vamos a ver es normativa ISACA

La Asignatura tiene dos vertientes:

- Conocer el '*control interno de informatica*'
- Conocer un poquito de auditoria informatica para lo que daremos una metodología de Auditoría.

## Definición

La auditoría es la revision independiente del control interno informatico.

Por ejemplo, el control interno informatico es **TODO**. Es la revision independiente de, por ejemplo, que los analistas programadores de una empresa siguen alguna metodologia adecuada.

## Organigrama

El modelo visto es un ejemplo que sigue normativa ISACA.

### – *Comite de Informatica*

Son los directores mas importantes, con principal importancia el director de informatica.

Este comite establece el '*plan informatico*' (obedeciendo a las necesidades del plan estrategico de la empresa y en pos de los objetivos que éste marque).

El hecho de que el plan estrategico se corresponda con el plan informatico es un control interno, por ejemplo.

El coordinador de este comité suele ser el director.

– *Director de sistemas informáticos*

Se podría unir al 'director del CPD' aunque algunos los separan por ser éste más organizativo.

– *USER TEAM*

Son expertos en el negocio que hacen de interface con los informáticos. Son por ejemplo unos intermediarios con conocimientos de derecho y de informática que intermedian entre un grupo de abogados y uno de programadores logrando así un mejor entendimiento.

– *Control de sistema*

Es un técnico de sistemas que sabe de sistemas y seguridad técnica.

El experto tiene que ser técnico de sistemas pues debe hacer de interfaz entre el SO y la seguridad lógica.

– *Garantía de calidad*

El organigrama no deja de ser una factoría de datos y software, hay un control de que ese software se produce como debe ser

– *Control de calidad de datos*

Es un control como el del software pero referido a los datos.

– *Centro de información*

Está obsoleto por la llegada de los pc's de gran capacidad de proceso.

Antes se copiaba del mainframe a ordenadores medios para dedicar el mainframe para los procesos prioritarios, las estadísticas sobre la empresa, eso era el centro de información que ya no existe.

– *Desarrollo y Mantenimiento*

Aquí es donde se hacen propiamente dichas las aplicaciones, con todo lo visto en la asignatura ingeniería del software.

– *Ofimática*

Mantenimiento de redes locales, aplicaciones ofimáticas, hardware, software etc...

– *Explotación*

– *Técnico de sistemas*

Agrupación de expertos de diversas modalidades como:

- Sistemas Operativos
- Sistemas Gestores de BBDD
- Telecomunicaciones

– *Centro de Atención al usuario*

Help Desk

Aquí entran todas las necesidades o problemas surgidos.

El 70% de los gastos informáticos están en mantenimiento

– *Captura de Datos*

Ya no se hace, ya no está centralizado sino que se hace por departamentos.

– *DataCenter*

Es donde están los ordenadores, servers o mainframes físicamente..

Contiene la planificación y organización de lo que se va a hacer a diario.

*La primera aplicación en cualquier empresa es la contabilidad y la 2ª es la nómina, la cual se sigue haciendo en batch*

*Existe software que gestiona automáticamente el helpdesk con prioridades, colas, etc... y lo manda a quien corresponda solucionar cada caso.*

### **Auditoria Informatica: Reglas de ORO**

- 1. Revision independiente del control interno informatico.
- 2. “*RIESGO VS CONTROL VS COSTE*”

En los sistemas de gestion hay riesgos, buscaremos controles que minimizen los riesgos y voy a ver que el coste del control no exceda el coste que supondria el propio riesgo.

### **Historia y Funciones del Aud. Informatico**

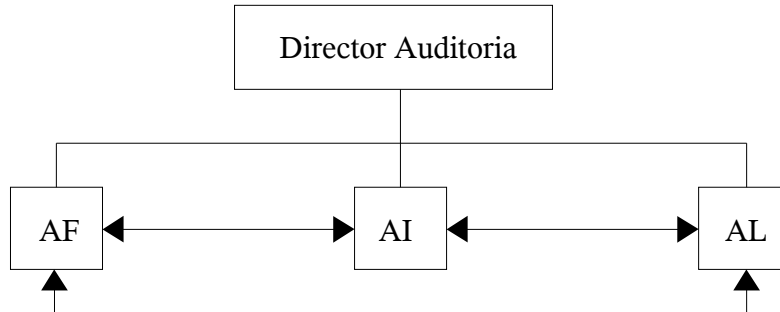
En el 69 nace la EDPAA = ISACA

En las empresas de esa epoca llegaban los auditores financieros, los cuales se preguntaron si la informacion que les daban los mainframes de esas empresas serian correctos o estarian manipulados. Nace pues el auditor informatico que entendia qué pasaba en el proceso de informacion.

Analistas programadores independientes que extraian informacion para el exterior. De ahí nace, de un apoyo al auditor financiero, aunque ahora mismo eso es lo menos importante de un auditor informatico, han surgido nuevas funciones:

- 1. *Analista programador para el auditor financiero.*
- 2. *Revision de controles internos informaticos genrales (seguridad logica, fisica, metodologias, estandares, etc...)*
- 3. *Revision de controles por area o departamento.*
- 4. *Revision de controles por aplicaciones (controles de entrada de informacion a la aplicacion, de proceso o de salida. Programacion).*
- 5. *Revision de controles de producto informatico (por ejemplo, como está instalado oracle, como lo tienen funcionando, revision de sistemas linux, unix, DB2 etc...)*
- 6. *Revision de aspectos legales.*

**Relaciones entre Auditoría informática, Auditoría Financiera y el auditor legal**

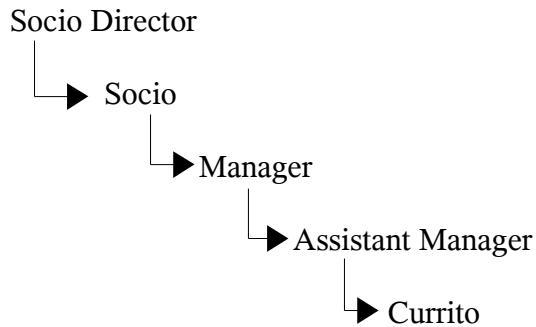


AF, AI y AL trabajan todos juntos.

**A. Externa**

Son empresas que se dedican a hacer auditoria.

Destacan *Delloite* (fusionada con *Arthur Andersen*), *KPMG*, *Ernst & Young*, *PriceWaterHouse* (las 4 grandes).



**A. Interna**

Un departamento interno que hace auditorias para ellos mismos.

Depende del comite directivo de la empresa.

**Metodologías de la Auditoría Informática**

Riesgo (vs) Control (vs) Coste

**1. Evaluación de Riesgos**

EDR, en ingles 'ROA' (la metodología) y fue creada por *Arthur Andersen (Risk Oriented Approach)*

Riesgos en los SI de todo tipo.  Seguridad logica, p.ej. (intrusismo)	1.....N	<u>Controles</u>  1. Existencia de paquete de seguridad logica.  2. Procedimiento de asignacion usuarios / password	<u>Prueba de cumplimiento</u>  El control existe y funciona.  Comprueba, verifica, determina y examina.  <i>Comprobar que los uarios tienen bien asignado su perfil</i>	<u>Prueba Sustantiva</u>  Es la ampliacion de la prueba de cumplimiento.  Por una falta de fiabilidad (de 6 usuarios comprobados 6 estan bien y 4 mal, p.ej), con esta prueba lo averigumos, examinando, p.ej a 100 usuarios.
---	---------	---	---	---

Objetivo de control

Esponer el riesgo en positivo y debe serlo ultimo y con tiempo. Si ya hemos hecho las pruebas y funciona, despues tratamos de ponerlo en positivo. Si el riesgo es 'el intrusismo', el objetivo es: 'los SI de informacion deben estar adecuadamente protejidos'

**2. Metodología *check-list* ó cuestionario**

<u>Prueba de cumplimiento</u>	<u>SI</u>	<u>NO</u>	<u>No Aplicable</u>
1. Comprobar que los extintores funcionan	X		
2. Comprobar que pasan la revision annual		X	

### 3. Metodología Producto

Sigue EDR pero con otro formato.

- I. Descripción de producto (*oracle 10.0 p.ej, se explica al lector como funciona esa base de datos*).
- II. Cuales son los riesgos del producto. (oracle en este caso)
- III. Controles que deben existir en oracle 10.0
- IV. Audit tools, Audit Trails, Audit Retrievals.

#### *Audit Tools*

Herramientas que hace oracle para hacer la auditoria.  
Comandos, etc...

#### *Audit Trails*

*Pistas de auditoria*, es un log del producto con lo que ocurre. El del S.O es el mas importante. Se explica como usarlo.

#### *Audit Retrievals*

Es un programa que se realiza "*llave en mano*", para extraer informacion que le interesa al auditor.

Normalmente lo hace el auditor.

### **Definicion de Auditoria de Ron Weber**

La auditoria informatica es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatico salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo los fines de la organizacion y utiliza eficazmente los recursos.

De esta forma la auditoria sustenta y confirma la consecuencia de los objetivos tradicionales de auditoría:

- Objetivos de certificacion de proteccion de activos e integridad de los datos (*enfoque de auditoria externa*)
- Objetivos de gestion que abarcan no solo los certificados sino tambien los de eficiencia y eficacia (*enfoque de auditoria interna*)

“Se puede concebir la auditoria informatica como una herramienta que ayuda a la organizaciones a un logro mayor de estos objetivos”

*Activos:*

- Personas
- Informacion, Datos
- Software
- Hardware

## Tipología de Controles

### Controles generales

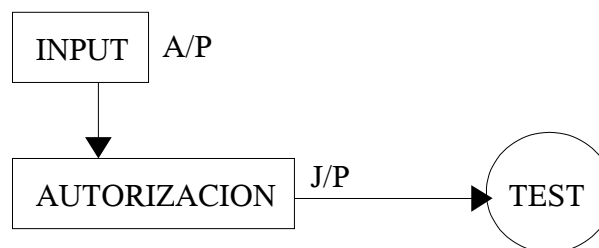
Son controles que aplican a todo el centro de proceso de datos, denominado hoy 'sistema de información'

1. Plan estratégico (vs) Plan Informático (*comite DSI de informática*).
2. Separación de entornos

<u>Entorno de desarrollo</u>	<u>Entorno de test</u>	<u>Entorno de Producción</u>
Donde están los analistas programadores y los jefes de proyecto haciendo programas. Aquí, en teoría, las BBDD son 'ficticias'.	Se prueban las aplicaciones creadas en el entorno de desarrollo. Aquí hay unos usuarios que la prueban al 100%	Aquí está el entorno real, datos y BBDD reales de la empresa.  AQUI NO SE JUEGA.

### Segregación de Funciones

Un ciclo completo no puede ser completado (valga la redundancia) por una sola persona, pero sí por dos.



En cualquier proyecto hay que pedir siempre 3 ofertas.

Aqui va la pagina 13 de las fotocopias del auditoria.

## **Fases de la Auditoria Informatica**

Las auditorias pueden ser sorpresivas o no sorpresivas asi como concertadas o no por la empresa que la recibe.

### **1. Definicion del alcance**

El alcance es lo que se va a revisar.

### **2. Recursos y Tiempo**

Planning para dividir la auditoria en (*dias/hombre*)

### **3. Recopilacion de informacion basica**

Antes de ir podemos pedir informacion como la estructura de su red por ejemplo, para llevar ya algo el primer dia, saber que nos vamos a encontrar, etc...

### **4. Programa de trabajo**

Planning para realizar la auditoria.

### **5. Conclusiones y comentarios**

Las observaciones o correcciones pueden ser *leves*, *medias* o *graves* y van a parar a un informe final que se discute con los managers, normalmente en una presentación (para facilitar su comprensión).

aquí va el formulario de los informes.

### Caso Práctico 1

- *Empresa: Lealtad Seguros.*
- *+1000 PC's en todas las capitales de provincia.*
- *El director general ha solicitado una auditoria de los PC's para ver si el control y gestion de los mismos se realiza de la forma adecuada, cumpliendo con las normas de la compañía y la de 'buenas practicas'*
  
- *No hay constancia de normas especificas del control y gestion de los PC's*
- *Los PC's nunca han sido auditados.*
- *Se considera que estan "stand alone". (Sin Red)*
- *Disponemos de un mes.*
  
- *Se solicita:*
  1. *Diseño del formulario de recojida de informacion.*
  2. *EDR de este caso.*