Resumen Final

Auditoría en Informática

Cristian Escudero
Basado en el resumen de Guido Ghisolfi

1 de noviembre de 2013

1. Control Interno y Auditoría Informática

1.1. Control Interno

Las `EMPRESAS-ACTIVIDADES-ORGANISMOS` a lo largo del tiempo van sufriendo **cambios**, a partir de la infuencia de **tendencias externas**: *globalización, avances tecnológicos, RR.HH., ideas, desafíos, ampliaciones/eliminaciones de ramas de negocio, fusiones con otras empresas.*

Ante la rapidez de los cambios, se requiere un buen `CONTROL` de todas las áreas y facetas de una empresa: *producción, procesos, flujo de información*, y *recursos* (humanos, materiales, etc).

> Se puede definir **control interno** como: «cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularides que puedan afectar al funcionanmiento de un sistema para conseguir sus objetivos.»

El **control** (actividad **continua** y **repetitiva**) se puede dar siempre que se sepa lo que se quiere, en base a:

- Normas.
- Estándares.
- Procedimientos.
- Objetivos deseados.

Su forma de incorporarlo subyace en dos opciones:

- En cada actividad en particular.
- Centralizado en un sector o área.

Los **tipos de control** que existen son:

- **Controles preventivos.** Para tratar de evitar el hecho (*ejemplo: software de seguridad que impide entradas no-autorizadas*).
- **Controles detectivos.** Cuando fallan los preventivos, para tratar de conocer cuanto antes el evento (*ejemplo: registro de intentos de acceso no-autorizados*).
- **Controles correctivos.** Facilitan la vuelta a la normalidad cuando se han producido incidencias (*ejemplo: recuperación de un archivo dañado a partir de una copia de seguridad*).

Los límites del **control** los brindará el `costo/beneficio` de la empresa en cuestión, ya que es una actividad diaria para la misma. Es responsabilidad de la Dirección plantear una estrategia de inversiones en recursos informáticos así como implantar sistemas de controles internos de manera que se garanticen unos grados de eficiencia y seguridad sufcientes de los activos informáticos.

1.2. Auditoría

> «Es la **actividad** consistente en la **emisión de una opinión profesional** sobre si el **objeto sometido a análisis** presenta **adecuadamente la realidad** que pretende **reflejar y/o cumple las condiciones** que le han sido prescriptas.»

Sólo tiene **validez** si la produce un profesional. Es llevada a cabo cuando existe una **alta incertidumbre** de como están siendo llevadas las cosas (surge ante las `necesidades`, `problemas` o `dudas` que se presenten), y se realiza a pedido (por alguien que necesite la opinión). Es una tarea *esporádica* o *frecuente*, cuyo **alcance** es el objeto a analizar.

> Una **auditoría** ataca a cualquier empresa, requiriendo saber en primera instancia cuáles son los *controles*.

1.2.1. Tipos de auditoría

Tipo	Objeto	Finalidad
Financieras	Registros contables.	Adecúan a la realidad.
Gestión	Toma de decisiones.	Eficaz, eficiente, económico.
Cumplimiento	Normas, disposiciones, procedimientos, legislación (NDPL).	Adecúan a las NDPL.
Informática	*Information Technology* (I.T.)	Eficiente y que se cumpla con NDPL.

Cada **tipo de auditoría** posee sus `procedimientos` para alcanzar el fin previsto.

1.3. Control Interno Informático (C.I.I.)

Controla **diariamente** que todas las actividades de I.T. son realizadas **cumpliendo los normas, estándares** y **procedimientos** (NEP), fijados por la **Dirección de la Organización** y/o la **Dirección de Informática**, así como los requerimientos legales.

El C.I.I. está dotado de las personas y medios materiales proporcionados a los cometidos que se le encomienden.

1.4. Auditoría informática (A.I.)

> «Proceso de **recolectar, agrupar y evaluar** `evidencias` para determinar si un `sistema informático` salvaguarda los **activos**, mantiene la **integridad de los datos**, lleva a cabo **eficazmente** los fines de la organización y utiliza **eficientemente** los recursos.»

Sistema informático: toda la tecnología del negocio. Todo lo que se maneja a través de la tecnología, no solamente el software.

1.4.1. C.I.I. y A.I.: campos análogos

Similitudes:

- Personal con conocimientos específicos en I.T.
- Verificación del cumplimiento de controles internos y NEP impuestos por la **conducción**.

Diferencias:

Control Interno Informático	***Auditoría Informática***
◦ Análisis de los controles en el día a día.	◦ Análisis de un **momento** informático determinado.
◦ Informa a la Dirección del Departamento de Informática.	◦ Informa a la Dirección General.
◦ Solo personal interno.	◦ Personal interno y externo.
◦ El alcance de sus funciones es únicamente sobre el Departamento de Informática.	◦ Tiene cobertura sobre todos los componentes de los *sistemas de información* de la organización.

1.4.2. Metodología de la A.I.

Conjunto de métodos para llevar adelante una A.I.:

1. **Definición del objeto de la auditoría.**
2. **Toma de contacto.** Conocer la organización, organigrama funcional, y conocer en detalle el sector de tecnología (*funciones, sectores, recursos humanos, tecnológicos y económicos*).
3. **Procedimientos y normas.** Desde el *acto de apertura de auditoría* al *acto de cierre.*
4. **Tipos de A.I.** Puede ser *completa*, sobre un determinado sistema, o una mezcla. Puede realizarse una comprobación de las acciones correctivas de auditorías anteriores.
5. **Realizar la/s auditoría/s.**
6. **Presentación de las conclusiones.** De forma simultánea o secuencial. De manera formal y/o visual (muestra los hallazgos de su trabajo a una audiencia).
7. **Soluciones alternativas a los problemas.** Es decir, proponer hacer algo en un cierto tiempo estimado bajo un determinado costo. Lo más importante es que sean soluciones adecuadas a la **realidad** de la empresa.

Nota: al hacer una A.I., hay que tratar de mantener objetividad y disciplina. Toda la actividad del auditor quedará reflejada en los `PAPELES DE TRABAJO`.

1.4.3. El Informe de Auditoría

Aspectos a tener en cuenta:

- **Normas.**
- **Evidencias.** La opinión debe estar basada en evidencias justificativas.
- **Irregularidades.** O sea, fraudes y errores. Es necesario diseñar pruebas antifraude.
- **Documentación.** El informe debe estar basado en los **papeles de trabajo**, o sea, a la totalidad de documentos preparados o recibidos por el auditor, que en conjunto constituyen un compedio de la información utilizada y de las pruebas efectuadas, juntos a las decisiones tomadas para llegar a formarse la opinión. Constituyen el conocimiento del auditor y pueden llegar a tener valor en el tribunal de justicia.

  Se incluye dentro de estos documentos: *el contrato entre el cliente y el auditor, las declaraciones de la dirección vinculadas con los objetivos a auditar, informes de terceras personas vinculadas al mismo.*
- **Informe.** Es la comunicación formal al cliente de: *alcances, resultados* y *conclusiones.*

Contenidos del informe:

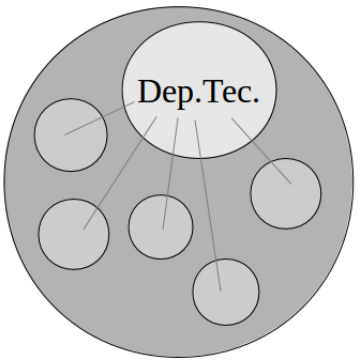
1. **Identificación del informe.** Título para distinguirlo de otros informes.
2. **Identificación del cliente.** Destinatario que solicita el trabajo.
3. **Identificación de la empresa a auditar.** Entidad objeto de la auditoría.
4. **Objetivos de la auditoría.** Para identificar su propósito, señalando los objetivos incumplidos.
5. **Normativas aplicadas y excepciones.** Todo lo que se tuvo en cuenta al realizar la A.I.
6. **Alcance auditoría.** Área organizativa, período de auditoría y limitación al alcance y restricciones del auditado.
7. **Conclusiones.** Informe corto de opinión, conteniendo los **puntos favorables** y **desfavorables**.
8. **Resultados.** Informe extenso, incluye plan de acción.
9. **Informes previos.** No es practica recomendable.
10. **Fecha del informe.** Inicio y fin del trabajo.
11. **Identificación y firma del auditor.**
12. **Distribución del informe.** Quienes podrán hacer uso del mismo.

2. Organización del Departamento de Auditoría Informática

2.1. Historia de la tecnología en las empresas

Hace sesenta años no existía la tecnología, el trabajo era manual y se almacenaba la información en papeles y registros. Con el surgimiento de la computación, el auditor tenía la necesidad de estudiar informática o contratar a un ayudante para que le brinde información. En la actualidad las empresas destinan importantes recursos en el sector tecnológico, volviéndose altamente dependientes del mismo, de tal forma que este domina su funcionamiento.

La tendencia futura de la auditoría informática radicará en los siguientes principios: todos los auditores deberán tener conocimientos informáticos; a la vez de mayor necesidad de especialistas con conocimiento cada vez más específico; y por último a la necesidad de un título profesional de auditor informático.



--

Figura 1: El Departamento Tecnológico es el que posee más recursos económicos y es denominado el "Corazón de la empresa". También denominado: Departamento tecnológico, Centro de cómputos o Dep de inf.

Para el buen funcionamiento del sector es necesario el **control interno**. Cuando surgen más problemas, lo recomendable es realizar una auditoría informática. En la actualidad, el auditor es experto en tecnologías y lo que antes era un auditor con un ayudante en tecnologías, ahora es un experto en tecnologías con ayudantes en las demás áreas: económicas, financieras, etc.

2.2. Perfil del Auditor Informático

Se deberán contemplar las siguientes características para mantener un profesional adecuado y actualizado:

1. Conocimiento básicos en:

- Desarrollo informático, gestión de proyectos y ciclos de vida de proyectos de desarrollo tecnológico.
- Gestión del departamento de tecnología.
- Análisis de riesgos en un entorno informático.
- Sistemas operativos.
- Telecomunicaciones.
- Gestión de base de datos.
- Redes locales.
- Seguridad física.
- Gestión de la seguridad y continuidad del negocio.
- Gestión de problemas y cambios.
- Administración de datos.
- Ofimática.
- Comercio electrónico.
- Encriptación de datos.

2. Técnicas de gestión empresarial y conocimientos financieros del negocio.
3. Conocimiento del concepto de Calidad Total.

2.3. Funciones a desarrollar por la Auditoría Informática

La función Auditoría Informática debe mantener en la medida de lo posible los objetivos de revisión que le demande la organización, abarcando campos de revisión como el C.I.I. de los servicios y de las aplicaciones.

> El **auditor informático** es responsable para establecer los OdC que reduzcan o eliminen la exposición al riesgo de control interno. El auditor deberá revisar los controles y evaluar resultados de su revisión para determinar correcciones y mejoras. Tiene además la obligación de proveer procedimientos y observaciones para mejorar la efectividad, eficacia y medición del riesgo empresarial.

3. Auditoría de la Dirección

Algunas actividades básicas de todo proceso de dirección son: *planificar, organizar, coordinar y controlar.*

3.1. ¿Cómo se debería trabajar en un Centro de Computo?

1. **Planificar** la conducción del área. Se trata de preveer la utilización de las I.T. en la empresa.
   - **Plan Estratégico de Tecnología** ó PEdT (proyectar a no más de tres años, ya que la tecnología cambia muy rápido). Tener en cuenta la situación actual, la cultura organizacional, el sector de la actividad y las acciones de la competencia. Debe asegurar el alineamiento de los *sistemas de información* con los objetivos en la empresa.
   - **Plan Operativo Anual.** Uno por cada año que se tenga planificado el PEdT. Se establece al comienzo de cada ejercicio y marca las pautas a seguir durante el mismo.
   - **Plan de Contingencia.** Contra algo que no esperamos que suceda y pueda ser de gran impacto, haciendo que peligre el funcionamiento de la empresa (*ejemplos: inundación, incendio, atentados, robos, ataques*). Ha de contener todo lo necesario para que permita la **continuidad** del negocio.
2. **Organizar y coordinar.** Sirve para estructurar los recursos, los flujos de información y los controles que permitan alcanzar los **objetivos** de la empresa.
   2.1. **Comité de informática.** En él debe haber representantes de todas las áreas usuarias y departamentos. Un auditor va a preguntar si existe un comité (si no, pedirá la creación de uno) y ver las decisiones tomadas por el mismo. Las funciones del comité son:

- Aprobación del PEdT.
- Aprobación de grandes inversiones en tecnología.
- Fijación de prioridades entre los grandes proyectos informáticos.
- Vehículo de discusión entre informáticos y sus usuarios.
- Vigilancia y seguimiento de la actividad del Departamento de Informática.

2.2. **Ubicación del Departamento de Informática en la empresa.** El auditor revisará su emplazamiento organizativo y su independencia de los otros departamentos.

2.3. **Descripción de funciones y responsabilidades del Departamento de Informática.** Funciones descritas y responsabilidades claramente delimitadas y documentadas. Ambas deben estar extendidas a todo el personal de informática. Además, ha de haber una **división entre funciones y responsabilidades**: se debe impedir que un solo individuo pueda transformar un proceso crítico. Entre las funciones, se listan:

- Administración de BD.
- A.I.
- C.I.I.
- Capacitación.
- Desarrollo.
- Mantenimiento.
- Redes.
- Seguridad.

2.4. **Estándares de funcionamiento y procedimientos.** Formentar, documentar y difundir. El auditor evaluará su existencia y adecuamiento (*por ejemplo, mediante entrevistas*).

2.5. **Gestión de recursos humanos.** El auditor revisará que sea llevado correctamente. Una forma es mantener estándares para:

- Proceso de selección: formalmente escrito.
- Evaluación de desempeño.
- Formación.
- Motivación.
- Promoción.
- Finalización de contrato.

2.6. **Comunicación**. Efectiva y eficiente entre Dirección de Tecnología y el personal.

2.7. **Gestión económica.**

- *Presupuestos económico:* que exista y sea adecuado, en línea con los planes estratégicos y operativos del Departamento.
- *Adquisición de bienes y servicios.*
- *Medida y reparto de costos:* evaluar su existencia y que este sea correcto.

2.8. **Seguros.** Tener cobertura para sistemas críticos o medir alternativas. Normalmente se aplica a empresas grandes.

3. **Controlar.** Efectuar un seguimiento **permanente** de las distintas actividades del Departamento de Tecnología, y que esté asegurado el **cumplimiento de la normativa legal** (ejemplos: *protección de datos personales, contratos de comercio electrónico, normativa emitida por órganos reguladores*).

4. Auditoría de la Seguridad Física

La `SEGURIDAD FÍSICA` **garantiza** la **integridad** de los activos humanos, lógicos y materiales de un **Centro de Cómputos**. Se deben tener medidas para atender los **riesgos de fallos**, local o general, según la **cronología del fallo** (antes, durante y después).

La **auditoría** es el medio que va a proporcionar la evidencia o no de la Seguridad Física en el ámbito en el que se va a desarrollar la labor profesional. La Auditoría Física no difiere de la auditoría general más que en el **alcance** de la misma.

4.1. Antes del fallo

Obtener y **mantener un nivel adecuado** de seguridad física sobre los activos. Ha tener en cuenta:

- Ubicación del edificio.
- Ubicación del Centro de Cómputos dentro del edificio.
- Compartimentación.
- Elementos de construcción. Perímetro físico.
- Potencia eléctrica. Generación de energía.
- Sistemas contra incendios.
- Control de acceso (ingreso/egreso).
- Selección del personal.
- Seguridad de los medios.
- Medidas de protección.
- Duplicación de medios.

4.2. Durante el fallo

Ejecutar un `PLAN DE CONTINGENCIA` adecuado. El mismo está formado por un **plan de recuperación ante desastres** más **un centro alternativo de cómputos**.

El plan de recuperación ante desastres debe:

- **Realizar un análisis de riesgos de sistemas críticos** (computadora, software, RR.HH.).
- Establecer un **período crítico** de recuperación.
- Realizar un análisis de aplicaciones críticas, **priorizando procesos**.
- Determinar las prioridades de procesos **por día** y su **orden**.
- Establecer objetivos de recuperación (*tiempo de interrupción*).
- Asegurar capacidad de comunicaciones y servicios de backups.

4.3. Después del fallo

Los contratos de seguros pueden compensar en mayor o menor medida las perdidas, gastos o responsabilidades que se puedan derivar una vez detectado y corregido el fallo.

Gama de seguros a contemplar:

- Cobertura por daño físico en los equipos.
- Reconstrucción de medios de software.
- Gastos extras (ejecución del plan de contingencia).
- Pérdida, robo, o daño de documentos y registros valiosos.
- Errores u omisiones de profesionales que ocasionen pérdidas.
- Cobertura de fidelidad con actos deshonestos o fraudulentos de los empleados.
- Transporte de medios ante perdida o daño en el transporte.
- Contratos con proveedores y de mantenimiento que aseguran **repuestos**.

4.4. Áreas de la Seguridad Física

Las áreas en las que el auditor ha de interesarse son:

- **Centro de proceso de datos e instalaciones.** Entorno, sala de Host, sala de Operadores, sala de Impresoras, cámara acorazada, oficinas, almacenes, instalaciones eléctricas, aire acondicionado, área de descaso y servicio.
- **Equipos y comunicaciones.** Host, terminales, computadoras personales, equipos de almacenamiento masivo de datos, impresoras, medios y sistemas de telecomunicaciones. Se ha de inspeccionar su **ubicación** y **acceso**.
- **Seguridad física del personal.** Accesos y salidas seguras, medios y rutas de evacuación, extinción de incendios, sistemas de bloqueo de puertas y ventanas. Normas y políticas emitidas y distribuídas al personal referente al **uso de instalaciones** por parte de éste.

4.5. Fuentes de la Auditoría Física

Para evaluar la Seguridad Física, las siguientes fuentes han de estar accesibles en todo CPD:

- Política, normas y planes de seguridad.
- Auditorías anteriores, generales y parciales.
- Contratos de seguros, de proveedores y de mantenimiento.
- Actas e informes de técnicos y consultores (edificio, electricidad, aire/calefacción).
- Informe de accesos y visitas.
- Informes sobre pruebas de evacuación.
- Políticas del personal.
- Inventario de soportes (backups, control de copias, etc).
- Inventario de tecnologías en general.

4.6. Herramientas y Técnicas del Auditor:

1. Observación
2. Lectura de documentación.
3. Entrevistas.
4. Consultas o asesoramientos.
5. Cámaras de video/fotográfica.
6. Cuaderno de campo/grabadora de audio.

4.7. Riesgos

- Ingresos no autorizados.
- Daños en los equipos.
- Atentados sobre equipos, instalaciones, documentación.
- Robos de equipos, documentos, sistemas, programas.
- Copiado y/o divulgación de información sensible.

4.8. Recomendaciones

- Instalaciones **claves**: ubicarse en lugares a los cuales no puede acceder el público.
- Edificios discretos y con señalamiento mínimos de su propósito.
- Equipamiento de soporte (fax, fotocopiadoras) deben ubicarse adecuadamente y controlar su acceso.

- Implementación de un sistema de detección de intrusos según estándares reconocidos.
- Materiales peligrosos o combustibles deben **almacenarse** en lugares seguros.
- Seguridad ambiental: analizar normativas referidas a comer, beber y fumar en áreas tecnológicas.
- Mantener **registro** de todas las **fallas** y de toda **actividad** vinculada con el mantenimiento preventivo y correctivo.
- Implementar controles cuando se retiran equipos de la sede de la organización para sus diversos fines.
- Considerar impacto de eventuales desastres en zonas próximas.
- Políticas de escritorio limpio: no dejar material que pueda ser confidencial (que pueda ser sustraído, robado, o fotocopiado).
- Política de pantallas limpias (dejar las mismas bloqueadas).
- Guardar bajo llave documentos y medios informáticos.
- **No** dejar conectadas PCs, terminales e impresoras al estar desatendidas.
- Proteger puntos de recepción y envío de fax/correo.

5. Auditoría del Desarrollo de Aplicaciones

La `INGENIERÍA DE SOFTWARE` (IS) puede ser entendida como el establecimiento y uso de **principios** de **ingeniería robustos**, orientados a obtener SW económico que sea fiable, cumpla los requisitos previamente establecidos y funcione de manera eficiente sobre la arquitectura esperada.

El `DESARROLLO` incluye **todo el ciclo de vida** del SW, excepto explotación, mantenimiento y la desafección o eliminación del mismo.

Para **auditar el desarrollo de aplicaciones** hay que verificar la existencia de controles internos que garanticen la construcción de SW basado en los **principios de IS**.

5.1. Importancia de la Auditoría del Desarrollo

- Los avances tecnológicos han hecho que el desafío mas importante y el principal factor de éxito de la informática sea la mejora de la **calidad del SW**.
- Gasto destinado a SW es cada vez mayor al dedicado al HW.
- El SW como producto es muy difícil de validar. A mayor control, mayor calidad y menor coste de mantenimiento.
- Hace unos años, se produjo la denominada "**crisis del SW**" (1970-1990). Estadísticas internacionales:
  - **1.5 %**: Se usó tal y como se entregó.
  - **3.0 %**: Se usó después de algunos cambios.
  - **19.5 %**: Se usó y luego se abandonó o se rehizo.
  - **47.0 %**: Se entregó pero nunca se usó.
  - **29.0 %**: Se pagó pero nunca se entregó.
- Aplicaciones informáticas pasan a ser un activo muy importante para la gestión.

5.2. Planteamiento y metodología

Las funciones que tradicionalmente se asignan al área de desarrollo son:

- Planificación del área y participación en la elaboración del PEdT.
- Desarrollo de nuevos sistemas.
- Estudios de **nuevos lenguajes**, técnicas, metodologías, estándares, herramientas relacionadas con el desarrollo y adopción de los mismos cuando sea oportuno para mantener un nivel de vigencia adecuado a la tecnología del momento.
- Establecer un plan de formación para el personal del área.
- Establecer normas y controles para las actividades del área y comprobar su observancia.

Se puede desglosar la auditoría del desarrollo en dos grandes apartados:

1. **Auditoría de la organización y gestión del área de desarrollo.**
2. **Auditoría de proyectos de desarrollo de sistemas de información.**

Partiendo de los riesgos potenciales que existen, se determinan una serie de **objetivos de control** (OdC) que los minimicen. Para cada OdC se han de especificar los controles que contribuyan a lograr su cumplimiento, junto a una serie de pruebas que comprueben la existencia y correcta aplicación de estos controles.

Una vez fijados los OdC, será función del auditor determinar el grado de cumplimiento de cada uno de ellos, y de los controles asociados.

5.3. Auditoría de la Organización y Gestión del Área de Desarrollo

Se consideran los siguientes objetivos de control:

1. El área de desarrollo debe tener **objetivos asignados** dentro del departamento y **una organización** que le permita el cumplimiento de los mismos.
2. El personal del área de desarrollo debe contar con la **formación** adecuada y estar **motivado** para la realización del trabajo.
3. Si existe un **plan de sistemas**, los proyectos que se lleven a cabo se basarán en dicho plan y lo mantendrán actualizado.
4. La propuesta y aprobación de nuevos proyectos debe realizarse de forma reglada.
5. La asignación de **recursos a los proyectos** debe hacerse de forma reglada.
6. El **desarrollo de sistemas de información** debe hacerse aplicando principios de la IS ampliamente aceptados.
7. Las **relaciones con el exterior** del departamento tienen que producirse de acuerdo a un procedimiento.
8. La **organización** del área debe estar **siempre adaptada** a las necesidades de cada momento.

5.4. Auditoría de Proyectos de Desarrollo de Sistemas de Información

La auditoría de un proyecto de desarrollo se puede hacer a medida que avanza el proyecto, o una vez finalizado el mismo. La diferencia es que en el primer caso el auditor puede afectar el desarrollo del mismo mediante sugerencias y observaciones.

Se consideran las siguientes fases dentro del desarrollo de S.I., en las cuales el auditor planteará los correspondientes OdC:

1. **Aprobación, planificación y gestión del proyecto.**
2. **Análisis.**
3. **Diseño.**
4. **Construcción.**
5. **Implantación.**