

# Auditoría del software

Adrián Riesco

Universidad Complutense de Madrid, Madrid, Spain

Auditoría, Calidad y Fiabilidad Informáticas 2022/23

# Auditoría del software

- 1 Introducción
- 2 Aspectos legales
- 3 El informe de auditoría
- 4 Normas técnicas de auditoría
- 5 Auditoría de la explotación
- 6 Auditoría de Internet
- 7 Auditoría de aplicaciones

# Contenidos

- En este tema veremos los conceptos básicos de lo que es una auditoría informática.
- Se debe tener en cuenta que la auditoría tiene muchos aspectos en común con las revisiones que se llevan a cabo para calidad.
- En este tema no repetiremos todos estos puntos, pero deben tenerse en cuenta en todo momento.
- Estudiaremos los aspectos más específicos.

# ¿Qué es la Auditoría Informática?

## Definición

*La Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.*

- No solo son necesarios auditores informáticos en el proceso de desarrollo de software, son necesarios en cualquier proceso en el que se *use* software.
- Esto incluye muchísimos campos, incluyendo partidos políticos, claros ejemplos de ausencia de auditorías en la actualidad.

# ¿Qué es la Auditoría Informática?

- Esta definición lo que hace es concretar los objetivos clásicos de la auditoría al caso de la informática:
  - Proteger los activos.
  - Objetivos de gestión, incluyendo eficiencia y eficacia.
- Las funciones de un auditor informático son:
  - Participar en las reuniones de diseño, implementación, etc.
  - Revisar y juzgar los controles para verificar que se ajustan a las órdenes de la dirección, pero también que cumplen los requisitos legales (como a las leyes de protección de datos).
  - Revisar y juzgar la eficacia, fiabilidad y seguridad de los equipos y el software.

# Audidores y revisiones internas

- En principio, los auditores cumplen funciones muy parecidas a las que hemos comentado en el tema anterior para los encargados de calidad.
- Estas similitudes son:
  - Son necesarios conocimientos especializados de Ingeniería del Software/Calidad.
  - Sus tareas son controlar que los productos se ajusten a las normas dadas por la compañía y por el cliente.
- De hecho, es habitual que alguien que trabaje en calidad reciba formación sobre auditoría y trabaje en ciertos casos como auditor (y viceversa).

# Audidores y revisiones internas

- Sin embargo, hay diferencias importantes:
  - El control interno se debe llevar a diario, mientras que las auditorías se realizan en fechas concretas.
  - Normalmente las auditorías las llevan a cabo personas externas (aunque es posible que sean internas).
  - Mientras que los encargados de calidad suelen trabajar para el departamento/sección informática, los auditores trabajan para toda la empresa.
  - Por esta razón, pueden trabajar (solicitar o auditar) con otros recursos que no son necesarios en la fase de calidad.
  - Muchas veces una auditoría externa puede encontrar problemas que el control interno puede tratar de **esconder**.
- Recordemos que, como vemos por las diferencias, los auditores pueden trabajar con el software en empresas no relacionadas en absoluto con el desarrollo del software, pero que hacen uso de él.

# Metodologías

- Los tipos de auditorías informáticas son:
  - Auditorías de controles generales.
  - Auditorías internas.
- El objetivo de las auditorías de controles generales es “dar una opinión sobre la fiabilidad de los datos del ordenador”.
- El resultado es un informe donde se citan los problemas encontrados.
- Normalmente estos informes están basados en cuestionarios estándar, y dan resultados muy generales.
- Suelen incluir una serie de pruebas y los resultados.



# Metodologías

- Para la auditoría interna se sigue un plan que cubre muchos más aspectos.
- En general, este plan incluye:
  - ① Identificar el área que se va a revisar, notificar al responsable y revisar los resultados de auditorías anteriores, si existen.
  - ② Identificar la documentación necesaria para revisar este área.
  - ③ Obtener información general del sistema, para reconocer los aspectos más importantes, que son los que deben ser auditados. Aquí se definen los objetivos de la auditoría.
  - ④ Obtener información detallada del sistema. Este proceso requiere entrevistas con el equipo a cargo del sistema.
  - ⑤ Identificación de los puntos críticos, es decir, aquellos en los que el riesgo es mayor.

# Metodologías

- ⑥ Ejecución de pruebas en los puntos críticos. Estas pruebas incluyen:
  - Cumplimiento de estándares y/o otras políticas.
  - Requisitos legales.
  - Prácticas generales de informática.
- ⑦ Evaluación de los resultados de las pruebas. Se buscan los problemas y se trata de explicar sus causas.
- ⑧ Generación del informe, que debe incluir sugerencias de mejora.

# El plan auditor

- El plan auditor informático es el documento en que se definen las funciones de la auditoría y el trabajo realizado.
- Su contenido debe estar coordinado con el resto de los planes auditores.
- Describe todo el trabajo realizado durante la auditoría hasta la entrega del informe final.
- El objetivo es ofrecer un plan para obtener los resultados esperados.

# El plan auditor

- El plan auditor debe incluir, al menos:
  - Tipo de auditoría que se está realizando, explicando los objetivos.
  - Procedimientos. Estos procedimientos incluyen qué incluir en el informe, cuándo y a quién entregarlo, cómo informar del inicio y del fin de la auditoría, la necesidad de informes preliminares, etc.
  - Sistema de evaluación. Se debe definir la escala que se va a usar (e.g. usaremos una escala de 0 a 10, donde 0 significa “absolutamente incorrecto” y 10 significa “absolutamente correcto”). También se debe indicar si se van a evaluar tareas a bajo nivel de detalle o aspectos más generales.
  - Nivel de exposición. El nivel de exposición es un valor entre 0 y 10 que resume la “calificación total” del sistema.
    - Dicho nivel depende de la puntuación del sistema, su importancia, las medidas que ya se estén tomando, etc.

# El plan auditor

- El plan auditor debe incluir, al menos (cont.):
  - Modos de seguimiento.
  - Plan de trabajo anual. Incluye los recursos necesarios para solucionar los problemas.
  - Plan quinquenal. Es necesario volver a realizar auditorías periódicamente, en general cada 5 años.
- El problema de todo este plan es que necesita de la experiencia del auditor, porque no es algo que se pueda hacer de manera sistemática.

# Aspectos legales

- ① Introducción
- ② Aspectos legales
- ③ El informe de auditoría
- ④ Normas técnicas de auditoría
- ⑤ Auditoría de la explotación
- ⑥ Auditoría de Internet
- ⑦ Auditoría de aplicaciones

# Aspectos legales en la auditoría informática

- A la hora de redactar un contrato de auditoría, hay varios aspectos legales que se deben tener en cuenta.
- Es importante comprobar que se están respetando todas las leyes.
- Esto puede no ser tan directo como puede parecer, dado el gran número de patentes que existen, o de los cambios en las leyes de protección de datos.
- En este punto vamos a dar una visión general de los aspectos legales que nos deben al menos sonar al hacer una auditoría.
- Se debe tener en cuenta que cada sistema es diferente, y que será necesario estudiar la legislación con cuidado (o contar con alguien que nos asesore) cuando realicemos una auditoría.

# Aspectos legales: Protección de datos

- La protección de datos es el aspecto legal más conocido en la informática.
- En España la Agencia Española de Protección de Datos (AEPD - <https://www.aepd.es/>) es la autoridad pública independiente encargada de velar por la privacidad y la protección de datos de los ciudadanos.
- Vela por el uso del Reglamento General de Protección de Datos (RGPD).
- El RGPD fue establecido por el Parlamento Europeo el 27 de abril de 2016.
- En aquellos aspectos que el RGPD no especifique ninguna norma se sigue la Ley Orgánica de Protección de Datos (LOPD - 1999).



# Aspectos legales: RGPD

- El RGPD cambia la mayoría de las normas.
- En especial quita atribuciones a la AEPD, ya que elimina el sistema de niveles de seguridad y la obligatoriedad de dar de alta los ficheros con datos personales.
- El RGPD tiene 3 principios básicos para regular la protección de datos:
  - El principio de responsabilidad proactiva de las empresas.
  - El principio del riesgo como referencia.
  - El principio de la protección de datos desde el diseño y por defecto.

# Aspectos legales: RGPD

- Las empresas deben ser responsables de las medidas de seguridad de los datos personales.
- Deben ser capaces de demostrar que están tomando las medidas adecuadas a sus clientes: tanto a personas individuales como a empresas.
- En particular, las compañías de desarrollo deben poder demostrárselo a sus clientes.

# Aspectos legales: RGPD

- Es también necesario **consentimiento explícito e inequívoco**.
- Deja de ser válido el consentimiento por omisión.
- El consentimiento por omisión obtenido en el pasado deja de ser válido.
- En el caso de menores, el consentimiento es válido a partir de los 16 años.
- Esta edad se da para servicios de la sociedad de la información (e.g. las redes sociales).
- No hay información al respecto en otros aspectos (como listas de correo), por lo que habrá que esperar a una ley española que lo regule.

# Aspectos legales: RGPD - Derechos

- El derecho al olvido.
- El derecho a la limitación del tratamiento de datos personales:
  - Suspensión temporal del tratamiento cuando se ha ejercitado el derecho de rectificación o de oposición.
  - Conservación de los datos cuando se va a proceder a la supresión de los datos y el interesado solicita en su lugar la limitación de los mismos para el ejercicio y defensa de reclamaciones frente a la AEPD.

# Aspectos legales: RGPD - Derechos

- El derecho a la portabilidad de los datos.
  - Se puede solicitar que una empresa reúna todos los datos sobre ti y se los traspase, en el formato adecuado, a otra empresa.
- El derecho a no ser sujeto de decisiones individuales automatizadas, incluyendo la elaboración de perfiles:
  - Tenemos derecho a que no se tomen decisiones totalmente automatizadas (sin intervención humana).
  - Las decisiones exclusivamente automatizadas están permitidas en los casos:
    - La decisión es necesaria para celebrar o ejecutar un contrato.
    - Está dado su consentimiento explícito.


# Aspectos legales: RGPD - Obligaciones


- La elaboración de contratos adaptados al RGPD.
- El registro del tratamiento, con información sobre:
  - ① El nombre y los datos de contacto del responsable.
  - ② Los fines del tratamiento.
  - ③ Las categorías de interesados y de datos personales.
  - ④ Las categorías de destinatarios de los datos personales
  - ⑤ Las transferencias de datos personales a un tercer país o una organización internacional.
  - ⑥ Los plazos previstos para la supresión de las diferentes categorías de datos.
  - ⑦ Una descripción general de las medidas técnicas y organizativas de seguridad aplicadas para garantizar la integridad y confidencialidad de los datos.
- El análisis de riesgos.

# Aspectos legales: RGPD - Obligaciones

- La AEPD proporciona ayuda con la herramienta FACILITA en el análisis de riesgos.
- Está dirigido a empresas con un nivel de riesgo bajo.

AGENCIA  
ESPAÑOLA DE  
PROTECCIÓN  
DE DATOS





HERRAMIENTA PARA  
TRATAMIENTOS  
DE ESCASO RIESGO

---

**Si su organización trata alguno de los datos de la lista, márkuelos:**

- ☐ Datos que revelen origen étnico o racial
- ☐ Datos de opiniones políticas o religión
- ☐ Datos de afiliación sindical (excepto cuotas sindicales)
- ☐ Datos genéticos
- ☐ Datos biométricos dirigidos a identificar de manera unívoca a una persona
- ☐ Datos de salud física o mental
- ☐ Datos relativos a la vida sexual o a la orientación sexual
- ☐ Datos relativos a condenas o infracciones penales
- ☐ Geolocalización
- ☐ Ninguno de los anteriores

<https://www.servicios.agpd.es/Facilita>

# Aspectos legales: RGPD - Obligaciones

- Una evaluación de impacto previa al tratamiento, si se da un tratamiento de datos con alto riesgo.
- El establecimiento de protocolos de actuación y/o recomendaciones para los usuarios y los responsables de los datos si ocurriera una violación de seguridad.
- La información debe estar:
  - Adaptada a la empresa.
  - Disponible siempre que sea necesaria.



# Aspectos legales: RGPD - DPD

- En ciertos casos es necesario que la empresa defina la figura del **delegado de protección de datos** (DPD).
- El DPD debe estar certificado como tal y se le valorará su dominio del área jurídica y de protección de datos en particular.
- Necesitan un DPD aquellas entidades:
  - Públicas.
  - Que tengan entre sus actividades principales el tratamiento de datos que requiera una observación habitual y sistemática de interesados a gran escala.
  - Que traten entre sus actividades principales datos sensibles a gran escala.
- Es decir, los autónomos y las Pymes que no cumplan alguna de las dos últimas no lo necesitan.
- La AEPD debe ser notificada del nombramiento de DPDs.

# Aspectos legales: RGPD - Sanciones

- El RGPD afecta a todas las personas físicas o jurídicas que gestionen información personal de un ciudadano de la Unión Europea.
- Esta obligación se aplica **estén los responsables en el territorio de la Unión o no**.
- Las sanciones expuestas por el Reglamento pueden llegar:
  - A los 20 millones de euros o al 4 % de la facturación global anual total para faltas muy graves.
  - A 10 millones o un 2 % para faltas graves.
  - No se especifica cuantía para las faltas leves.

# Aspectos legales: RGPD - Sanciones

Para establecer la gravedad se tendrá en cuenta:

- La naturaleza, gravedad y duración de la infracción, así como el número de interesados afectados.
- La intencionalidad o negligencia en la infracción.
- Cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados.
- El grado de responsabilidad del encargado del tratamiento de los datos, habida cuenta de las medidas técnicas u organizativas que se hayan aplicado.
- Toda infracción anterior cometida.
- El grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción.

# Aspectos legales: RGPD - Sanciones

Para establecer la gravedad se tendrá en cuenta (continuación):

- Las categorías de los datos de carácter personal afectados por la infracción.
- La forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida.
- Que el responsable, en relación con el mismo asunto, ya haya sido sancionado, entre otras, con una advertencia o apercibimiento al cumplimiento de dichas medidas.
- La adhesión a códigos de conducta o a mecanismos de certificación aprobados con arreglo al articulado del propio RGPD.
- Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

# Aspectos legales: La protección jurídica del software

- La clasificación jurídica del software es compleja, porque ciertos aspectos caen bajo la legislación de propiedad industrial y otros bajo la de propiedad intelectual.
- La “Ley Sinde”, que en principio formaba parte de la Ley de Economía Sostenible y que finalmente fue aprobada en marzo de 2012, ha generado mucho debate considerando el software desde el segundo punto de vista.
- Por otro lado, tenemos las licencias que ayudan a los usuarios a no ejercer todos los derechos de propiedad intelectual que les permite la ley.
- En este caso podemos usar, por ejemplo, las licencias de Creative Commons o GPL.

# Aspectos legales: La protección jurídica del software

- Creative Commons permite distinguir ciertas condiciones:



**Reconocimiento (Attribution):** En cualquier explotación de la obra autorizada por la licencia hará falta reconocer la autoría.

---



**No Comercial (Non commercial):** La explotación de la obra queda limitada a usos no comerciales.

---



**Sin obras derivadas (No Derivate Works):** La autorización para explotar la obra no incluye la transformación para crear una obra derivada.

---



**Compartir Igual (Share alike):** La explotación autorizada incluye la creación de obras derivadas siempre que mantengan la misma licencia al ser divulgadas.

<http://es.creativecommons.org/blog/licencias/>

# Aspectos legales: La protección jurídica del software

- Con estas condiciones se pueden generar las seis combinaciones que producen las licencias Creative Commons:



**Reconocimiento (by):** Se permite cualquier explotación de la obra, incluyendo una finalidad comercial, así como la creación de obras derivadas, la distribución de las cuales también está permitida sin ninguna restricción.



**Reconocimiento – NoComercial (by-nc):** Se permite la generación de obras derivadas siempre que no se haga un uso comercial. Tampoco se puede utilizar la obra original con finalidades comerciales.



**Reconocimiento – NoComercial – CompartirIgual (by-nc-sa):** No se permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.



**Reconocimiento – NoComercial – SinObrasDerivadas (by-nc-nd):** No se permite un uso comercial de la obra original ni la generación de obras derivadas.



**Reconocimiento – CompartirIgual (by-sa):** Se permite el uso comercial de la obra y de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.



**Reconocimiento – SinObrasDerivadas (by-nd):** Se permite el uso comercial de la obra pero no la generación de obras derivadas.

<http://es.creativecommons.org/blog/licencias/>

# Aspectos legales: La protección jurídica del software

- El problema de las licencias Creative Commons es que no tiene en cuenta el software en particular, por lo que no tiene en cuenta aspectos particulares del código y su reutilización.
- Para tener en cuenta el código podemos usar licencias GPL.
- GPL significa **Licencia Pública General** (General Public License).
- Su propósito es declarar que el software cubierto por esta licencia es software libre y protegerlo de intentos de apropiación que restrinjan esas libertades a los usuarios.



## Aspectos legales: La protección jurídica del software

- En cualquier caso, el auditor tiene que asegurarse de que se cumplan los términos de la licencia del software utilizado.
- Para ello tiene que estudiar si es posible que se use software “pirateado”.
- Es necesario estudiar las posibles violaciones de licencias, el coste que supone y el coste que supondría investigar cada aplicación y cada ordenador individualmente.
- Hay métodos generales para llevar un inventario del software en toda la empresa y cuestionarios para hacer “auto-auditorías”.
- Con ello se intenta concienciar a las empresas de la necesidad de evitar este tipo de fraude.

# Aspectos legales: La protección jurídica de las bases de datos

- Dado que una base de datos contiene datos pero proporciona información, se considera que entra dentro de la protección de la propiedad intelectual.
- Pero además se considera en general que las bases de datos deben ser protegidas por más motivos, porque se ha invertido dinero para:
  - obtener los datos.
  - diseñar la base de datos.
  - definir los algoritmos para recopilar la información de una determinada manera.
  - comprar el hardware necesario para almacenarla.
- Por ello, es necesario defender tanto a los “dueños” de los datos almacenados como a los programadores.

# Aspectos legales: La protección jurídica de las bases de datos

- La auditoría debe, por tanto, comprobar que:
  - Comprobar los métodos de adquisición de datos.
  - Comprobar que el diseño es correcto.
  - Se protegen los datos y los autores de la base de datos.
  - Se evitan las copias no autorizadas.
  - La base de datos se gestiona adecuadamente.
  - Para ello, es posible que debamos comprobar la formación del personal.

# Aspectos legales: Contratación electrónica

- Contratación electrónica es toda aquella que se realiza por algún medio electrónico, en general por Internet.
- Se suele hablar de 3 tipos de contratación:
  - Empresa-consumidor final (*business to consumer*, B2C).
  - Empresa-empresa (*business to business*, B2B).
  - Empresa-administraciones públicas (*business to administrations*, B2A).
- Páginas como *ebay* han creado un nuevo tipo, consumidor-consumidor (*consumer to consumer*, C2C).

# Aspectos legales: Contratación electrónica

- También se distingue entre comercio electrónico directo e indirecto.
- Por comercio directo nos referimos a obtener un bien o servicio íntegramente en el medio electrónico.
- Un ejemplo de este caso es la compra en línea de un libro en formato electrónico, como *epub*.
- El comercio indirecto implica una acción que no se realiza de forma electrónica.
- Un ejemplo típico sería comprar un libro “en papel”.
- Pero otro ejemplo sería comprar un libro electrónico que se envía al domicilio en una memoria usb.

# Aspectos legales: Contratación electrónica

- En la contratación electrónica hay que atender a 3 aspectos fundamentales:
  - Momento en el que se considera que se ha llegado a un acuerdo (al hacer una oferta, al ser aceptada, etc.)
  - La calidad del diálogo (videoconferencia, email, página web, etc.).
  - La seguridad.
- Este último aspecto es en el que nos centraremos.
- En las transmisiones electrónicas buscamos garantizar la autenticidad, la integridad (i.e. la transmisión llega) y el no repudio (en origen y destino) de las mismas.
- En España ahora se puede hacer esto con la firma electrónica.

# Aspectos legales: Contratación electrónica

## Discusión

*En un intento por protegerse de la piratería, los libros electrónicos cuentan con una protección en general y, en mi opinión, excesiva. En general, al comprar un libro electrónico necesitas un programa específico para descargarlo y tener la suerte de tener un lector compatible con dicho programa. ¿Crees que este es el mejor medio para promocionar este medio?*

# Aspectos legales: Contratación electrónica

- En España existe la Ley 59/2003, de Firma electrónica, que define tres tipos de firma:
  - Simple.** Datos que puedan ser usados para identificar al firmante (autenticidad).
  - Avanzada.** Además de identificar al firmante permite garantizar la integridad del documento y la integridad de la clave usada. Utiliza para ello un DSCF (dispositivo seguro de creación de firma, el DNI electrónico).
  - Reconocida.** Es la firma avanzada y amparada por un certificado reconocido (certificado que se otorga tras la verificación presencial de la identidad del firmante). También se conoce como cualificada, por la traducción de *qualified*.



# Aspectos legales: Contratación electrónica

- En estos casos es importante contar con asesores jurídicos, puesto que prácticas muy recientes y la legislación cambia frecuentemente.
- Los aspectos a tener en cuenta son:
  - Delimitación de responsabilidades.
  - Garantías.
  - Reparto de obligaciones entre distintos países.

# Aspectos legales

YOUTUBE &gt;

## El niño de 12 años que se gastó 100.000 euros en YouTube

Un menor alicantino contrata publicidad al intentar ganar dinero con su canal de YouTube. La historia muestra el riesgo de aceptar sin leer las condiciones de un servicio en Internet



MANRIQUE C. SÁNCHEZ | JAVIER PEDREIRA 'WICHO' | MICROSIERVOS

Alicante / Madrid - 4 OCT 2016 - 19:50 CEST

[http://tecnologia.elpais.com/tecnologia/2016/10/04/actualidad/1475578401\\_460930.html](http://tecnologia.elpais.com/tecnologia/2016/10/04/actualidad/1475578401_460930.html)

# Aspectos legales

WHATSAPP ›

## WhatsApp consume su advertencia: o se aceptan sus condiciones o no se podrá seguir usando

La compañía cambió su política al compartir los datos de sus usuarios con Facebook



JOSÉ MENDIOLA ZURIARRAIN

27 SEP 2016 - 19:58 CEST

[http://tecnologia.elpais.com/tecnologia/2016/09/27/actualidad/1474975944\\_468987.html](http://tecnologia.elpais.com/tecnologia/2016/09/27/actualidad/1474975944_468987.html)

# Aspectos legales: Contratación informática

- La contratación informática se refiere a la compra de bienes o servicios informáticos, incluyendo software y hardware.
- No existe una calificación uniforme para asignarle un tipo estándar de contrato.
- Esto se debe tanto a las grandes diferencias entre hardware y software como al desconocimiento en general de las posibilidades de los equipos (en general se tiene más claro qué tipo de estantería quieres que qué tipo de ordenador quieres).
- Muchas veces se crea sencillamente un contrato al que se adhiere el cliente, sin posibilidad de modificaciones.
- El auditor debe asegurarse de que las cláusulas son justas para cualquier potencial cliente.

# Aspectos legales: Transferencia electrónica de fondos

- La transferencia electrónica de fondos está muy ligada a la contratación electrónica.
- Sin embargo, tiene tanta importancia que se le da un trato separado.
- De nuevo, es necesario asesoramiento legal específico.
- El auditor simplemente comprueba que las tarjetas pueden ser leídas por el hardware, y la existencia de redes adecuadas.
- **Posible tema:** dinero electrónico como BitCoin.

## Aspectos legales: Subcontratas

- La externalización de la gestión no supone que el empresario pierda el control sobre la administración del sistema.
- Simplemente que se lo encarga a un tercero para ahorrar costes.
- Suele ser habitual y aconsejable que las empresas incluyan en los contratos una cláusula en virtud de la que podrán realizar una auditoría de los procedimientos que el subcontratado está siguiendo.
- La auditoría debe garantizar que se siguen los acuerdos pactados entre las partes.

# Aspectos legales: El delito informático

- Hay muchos tipos de delitos informáticos.
- El fraude es el más importante de ellos.
- Otros delitos importantes son:
  - Los virus.
  - El “pirateo informático” (hackers y atentados contra la propiedad intelectual).
  - El robo.
- El auditor debe controlar que no se estén dando ninguno de estos delitos.

# El informe de auditoría

- 1 Introducción
- 2 Aspectos legales
- 3 El informe de auditoría**
- 4 Normas técnicas de auditoría
- 5 Auditoría de la explotación
- 6 Auditoría de Internet
- 7 Auditoría de aplicaciones



# El informe de auditoría

- El informe de auditoría constituye el producto final del trabajo de auditoría y la única documentación que se va a entregar.
- Sus objetivos son:
  - Permitir al que revisa entender el trabajo realizado, las circunstancias que afectan a su fiabilidad y las conclusiones del auditor.
  - Prevenir una interpretación errónea del grado de responsabilidad asumido por el auditor.
- El informe debe ir firmado.

# El informe de auditoría

- Un informe debe constar de las siguientes partes:
  - Título.
  - Destinatario.
  - Identificación de la entidad auditada.
  - Párrafo de alcance.
  - Párrafo de comparabilidad (con ejercicios anteriores).
  - Párrafo de salvedades (indicando su efecto en el informe).
  - Descripción de los incumplimientos (incluyendo motivos y recomendaciones).

# El informe de auditoría

- Un informe debe constar de las siguientes partes (cont.):
  - Párrafo de énfasis.
  - Párrafo sobre el informe de la gestión.
  - Resumen en términos no técnicos.
  - Decisión final.
  - Firmas y fecha.
- Para que el informe se transmita de forma satisfactoria es necesario que el documento pueda ser leído y comprendido sin dificultad.
- Es mejor añadir explicaciones extra que abusar de concisión.

# El informe de auditoría

- La descripción de los incumplimientos es especialmente importante.
- En cada punto debe indicarse la razón por la que es un incumplimiento y alguna recomendación.
- Ha de discutirse con los auditados antes de emitir el definitivo.
- En algunas ocasiones se pueden recoger también estas discusiones.

# Informes

- Según los resultados del trabajo los tipos de opiniones básicas son cuatro:
  - Favorable.** Se concluye que el sistema es satisfactorio.
  - Desfavorable.** Se considera que el sistema no es aceptable.
  - Con salvedades.** El sistema es satisfactorio, aunque contiene ciertas debilidades o incumplimientos que no llegan a invalidarlo.
  - Denegación de opinión.** El auditor no tiene suficientes elementos de juicio para poder opinar.

# Informes

- Cuando el auditor detecte debilidades durante la realización de la auditoría debe comunicarlas al cliente a la mayor brevedad posible.
- Un esquema general de cómo presentar las debilidades es el siguiente:
  - 1 Describir la debilidad.
  - 2 Indicar el criterio de medida que se ha utilizado.
  - 3 Indicar los efectos que puede tener en el sistema.
  - 4 Describir la recomendación con la que esa debilidad se podría eliminar.
  - 5 Respuesta de los directivos.

# Normas para elaborar los informes

- La elaboración y el contenido de los informes de auditoría deben ajustarse a las **Normas de Auditoría de Generalmente Aceptadas** (NAGA).
- Estas normas generales se pueden resumir como:
  - ① El trabajo de auditoría debe planificarse apropiadamente y, si existen ayudantes, se supervisará adecuadamente su labor.
  - ② Debe efectuarse un estudio y evaluación del sistema de control interno existente para conocer su fiabilidad y determinar el alcance, naturaleza y momento de aplicación de los procedimientos de auditoría.
  - ③ La cantidad y calidad de evidencia debe obtenerse mediante la aplicación de los procedimientos de auditoría que proporcionen una base de juicio razonable.

# Normas para elaborar los informes

- Más concretamente, las NAGA están constituidas por un grupo de 10 normas adoptadas por el [American Institute of Certified Public Accountants](#).
- Las normas tienen que ver con la calidad de la auditoría realizada por el auditor independiente.
- Se dividen en 3 grupos:
  - ① Normas generales.
  - ② Normas de la ejecución del trabajo.
  - ③ Normas de información.



# Normas para elaborar los informes

- Las **normas generales** son:

**Entrenamiento y capacidad profesional.** La auditoría la realizará una persona o personas que tengan una formación técnica adecuada y competencia como auditores.

**Independencia.** En todos los asuntos concernientes a ella, el auditor o los auditores mantendrán su independencia.

**Cuidado o esmero profesional.** Debe ejercerse el debido cuidado profesional al planear y efectuar la auditoría y al preparar el informe.

# Normas para elaborar los informes

- Las normas de la ejecución del trabajo son:

**Planeamiento y Supervisión.** El trabajo se planeará adecuadamente y los asistentes, si los hay, deben ser supervisados rigurosamente.

**Estudio y Evaluación del Control Interno.** Se obtendrá un conocimiento suficiente del control interno, a fin de planear la auditoría y determinar la naturaleza, el alcance y la extensión de otros procedimientos de la auditoría.

**Evidencia Suficiente y Competente.** Se obtendrá evidencia suficiente y competente mediante la inspección, la observación y la confirmación, con el fin de tener una base razonable para emitir una opinión respecto a los estados financieros.

# Normas para elaborar los informes

- Las normas de información son:

**Aplicación de los Principios de Contabilidad Generalmente Aceptados.** El informe indica si los estados financieros están presentados conforme a los principios de contabilidad generalmente aceptados.

**Consistencia.** El informe especificará las circunstancias en que los principios no se observaron consistentemente en el periodo actual respecto al periodo anterior.

**Revelación Suficiente.** Las revelaciones informativas se considerarán razonablemente adecuadas, salvo que se especifique lo contrario en el informe.

**Opinión del Auditor.** El informe contendrá una expresión de opinión o una aclaración de que no puede expresarse una opinión. En este último caso, se indicarán los motivos. En los casos en que el nombre de auditor se relacione con los estados financieros, el informe incluirá una indicación clara del tipo de su trabajo y del grado de responsabilidad que va a asumir.

# Normas para elaborar los informes

- Seguir las normas facilita la comparación de los informes realizados por distintos auditores.
- A la hora de preparar el informe, el auditor debe tener en cuenta las necesidades y características de los destinatarios.
- El informe debe contener un párrafo en el que se indiquen los objetivos que se pretenden cumplir.
- Si algún objetivo no se puede alcanzar se debe indicar en el informe.
- Se debe también indicar cuáles son las NAGA que se han seguido.

# Normas para elaborar los informes

- Igualmente, es necesario incluir las excepciones de seguimiento de estas normas, el motivo de no seguirlas y, si procede, los efectos que puede tener en la auditoría.
- Como ya hemos comentado, se ha de hacer mención del alcance de la auditoría y se debe describir la naturaleza y la extensión del trabajo de auditoría.
- En el alcance se indican las circunstancias que hayan limitado el alcance.
- El informe incluye toda la información sobre las debilidades.

# Normas para elaborar los informes

- También se debe incluir la opinión del auditor sobre el área auditada.
- En función de los objetivos, esta opinión puede ser general y referirse a todas las áreas.
- El informe debe presentarse de una forma lógica y organizada.
- Debe contener la información suficiente para ser comprendido por el destinatario, de tal manera que puede llevar a cabo las correcciones necesarias.
- El informe se debe emitir en el momento más adecuado para que permita las acciones.
- Antes de emitir el informe se pueden ir dando instrucciones a personas/grupos concretos.

# Auditoría del software

- 1 Introducción
- 2 Aspectos legales
- 3 El informe de auditoría
- 4 Normas técnicas de auditoría
- 5 Auditoría de la explotación
- 6 Auditoría de Internet
- 7 Auditoría de aplicaciones

# Normas técnicas de auditoría

- Las normas técnicas son los requisitos que el auditor debe cumplir en el ejercicio de sus funciones para expresar su opinión técnica y responsable.
- Las normas técnicas se clasifican según el grado de obligación:
  - Principios.** Aquellas requisitos de obligado cumplimiento.
  - Directivas.** Guías para realizar la auditoría, pero que dependen del juicio del auditor para ser aplicadas. De no hacerlo, se deben justificar.
  - Procedimientos.** Ejemplos de cómo realizar la auditoría. No son de obligado cumplimiento.
- Nos centraremos en los principios, dado que es obligatorio seguirlos.



# Principios de auditoría: Formalidad

- El primer principio de auditoría es la **formalidad**.
- Incluye la responsabilidad, las atribuciones y las obligaciones.
- En el caso de auditoría interna deben documentarse de manera formal en unos estatutos.
- En el caso de auditoría externa se deben documentar formalmente en una carta de encargo o contrato.

# Principios de auditoría: Independencia

- El segundo principio de auditoría es la **independencia**.
- Por un lado tenemos la *independencia profesional*.
- El auditor de sistemas de información debe ser independiente de la organización auditada.
- Por otro lado, tenemos la *relación con la organización*
- La función de auditoría debe ser lo suficientemente independiente del área que se esté auditando para permitir realizar de manera objetiva la auditoría.

## Ejemplo

*Un auditor no puede ser un directivo de una compañía rival, que esté interesado en que los resultados de sus competidores sean lo peor posibles.*

# Principios de auditoría: Ética y normas profesionales

- El siguiente principio se dedica a la *ética y las normas profesionales*.
- Primero tenemos el *código de ética profesional*.
- Distintos organismos han publicado códigos de conducta o normas que el auditor de sistemas ha de cumplir.
- Además tenemos la *Diligencia profesional*.
- En todos los aspectos del trabajo del auditor se debe ejercer la atención profesional correspondiente y el cumplimiento de las normas aplicables de auditoría profesional.

## Ejemplo

*Si por razones de causa mayor el auditor no cumpliera los principios de independencia, se espera de él que trabaje de manera justa y no se deje llevar por sus intereses.*

# Principios de auditoría: Ética y normas profesionales

≡ EL PAÍS 

ECONOMÍA

ECONOMÍA EMPRESAS MERCADOS BOLSA MIS AHORROS VIVIENDA TECNOLOGÍA OPINIÓN/ANÁLISIS BLOGS EMPLEO FORMACIÓN TITULARES »

## Multa y despido para la auditora que se enamoró de su cliente

EE UU sanciona a EY con 9,3 millones de dólares por las 'relaciones peligrosas' con directivos de empresas auditadas

[http://economia.elpais.com/economia/2016/09/19/actualidad/1474305828\\_264250.html](http://economia.elpais.com/economia/2016/09/19/actualidad/1474305828_264250.html)

# Principios de auditoría: Idoneidad

- El siguiente principio se refiere a la **idoneidad**.
- Primero debemos estudiar las *habilidades y conocimientos*.
- El auditor debe ser técnicamente idóneo y tener la experiencia y los conocimientos necesarios para realizar su trabajo.
- Además, se debe tener en cuenta la *formación profesional continua*.
- El auditor debe mantener la idoneidad técnica mediante su formación continua.

# Principios de auditoría: Planificación

- El siguiente principio es el de **planificación**.
- El auditor debe planificar el trabajo para:
  - Satisfacer los objetivos de la auditoría.
  - Cumplir con las normas aplicables a la profesión.

# Principios de auditoría: Ejecución de la auditoría

- El sexto principio está dedicado a la *ejecución de la auditoría*.
- Primero debemos estudiar la *evidencia*.
- El auditor debe tener evidencia adecuada (fiable, relevante y útil) y suficiente para lograr los objetivos.
- Los hallazgos y conclusiones de la auditoría se deben basar en el análisis de dicha evidencia.
- También debemos preocuparnos de la *documentación*.
- La auditoría debe documentarse, describiendo las labores realizadas y la evidencia que respalda los hallazgos y conclusiones del auditor.
- Por último, tenemos la *supervisión*.
- El personal de auditoría debe ser supervisado para tener una garantía razonable de que se lograrán los objetivos.

# Principios de auditoría: Información

- El último principio es el de **información**.
- Este principio se refiere al *contenido y formato de los informes*.
- Al terminar el informe, el auditor debe proporcionar un informe con un formato apropiado a los destinatarios.
- Como hemos visto, el informe debe enunciar el alcance, objetivos, restricciones, autores, resultados, recomendaciones, etc.



# Los servicios del auditor

- Los tipos de servicios que un auditor puede prestar se agrupan en las categorías:
  - Auditoría.
  - Revisión limitada.
  - Hechos concretos (o procedimientos acordados).

# Auditoría y revisión

- La auditoría proporciona un nivel alto, pero no absoluto, de seguridad sobre la eficiencia de los procedimientos de control.
- Esta conclusión se conoce por **expresión positiva de seguridad**.
- La seguridad absoluta es difícil de conseguir debido a factores como la necesidad del juicio profesional, la realización de más pruebas y otras limitaciones.
- La revisión limitada es una “versión light” de la auditoría.

# Auditoría y revisión

- Proporciona un nivel moderado de seguridad sobre la efectividad de los procedimientos.
- El nivel de seguridad es menor debido a que el alcance es de menor amplitud y que la naturaleza y la extensión de los procedimientos no permiten obtener evidencia tan concluyente como en la auditoría.
- El objetivo de la revisión es permitir al auditor declarar si, con la evidencia obtenida, nada ha llegado a su conocimiento que le induzca a pensar que los procedimientos no son efectivos.
- Esta conclusión se conoce por **expresión negativa de seguridad**.

# Auditoría y revisión

- Tanto la auditoría como la revisión limitada suponen:
  - Planificar el encargo.
  - Evaluar la efectividad del diseño de procedimientos de control.
  - Realizar pruebas sobre la efectividad operativa de los procedimientos de control (el tipo y extensión de las pruebas depende de que estemos en una auditoría o en una revisión).
  - Formarse una opinión e informar basándose en los criterios identificados:
    - La conclusión de una auditoría se expresa con una opinión positiva y proporciona un nivel de seguridad alto.
    - La conclusión de una revisión se expresa con una opinión negativa y proporciona un nivel de seguridad bajo.
    - Obviamente, es posible encontrar problemas en ambos casos, lo que supondrá listarlos en el informe.

# Hechos concretos o procedimientos acordados

- En la auditoría de hechos concretos el auditor no concluye con ninguna expresión de seguridad.
- Al auditor se le encarga que realice unos procedimientos específicos para cubrir las necesidades de información de partes específicas.
- El auditor emite un informe para estas partes.
- Los receptores del informe extraen sus propias conclusiones.
- El uso del informe queda restringido a las personas que se encargaron del acuerdo, ya que otras personas podrían malinterpretar los resultados al no conocer las razones por las que se solicitaron.

# Ciclo de vida

- El proceso de auditoría implica diversas etapas en las que el auditor ha de seguir cumpliendo las normas para poder emitir una opinión profesional sobre el sistema.
- Para realizar este trabajo se utilizan una serie de métodos y herramientas.
- En los métodos se indica la secuencia en las que se deben realizar los distintos pasos de la auditoría.
- Esta secuencia es el **ciclo de vida** o **metodología**.
- Este ciclo de vida es similar al método de desarrollo en espiral.

# Ciclo de vida

- Utilizar un determinado ciclo de vida para auditar un sistema permite:
  - Definir las actividades necesarias.
  - Evaluar riesgos.
  - Determinar los recursos a asignar.
  - Especificar la secuencia de las actividades.
  - Establecer puntos de control.
  - Obtener información para mejorar el sistema de auditoría.
  - Reflejar los resultados parciales y finales.
- El ciclo de vida consta de una fase inicial y otra final.
- Entre ambas se da un ciclo de 4 fases.

# Ciclo de vida

## ① Inicio

- La fase de inicio consiste en una entrevista con los responsables del sistema.
- Se debe solicitar un inventario de los recursos del sistema.
- De esta manera se estima la extensión del sistema.
- Con esta estimación se da el presupuesto.

## ② Planificación

- Esta fase se usa para asegurarse de que:
  - El alcance y el contexto de la auditoría se ha establecido correctamente.
  - Todos los riesgos se han identificado y cuantificado.
  - Se asignan los recursos necesarios para que se pueda realizar la auditoría.
  - Se ha desarrollado un plan para tratar adecuadamente los riesgos.
- La actividad del plan se documenta para facilitar la gestión de la auditoría.



# Ciclo de vida

## ③ Ejecución

- En esta fase se llevan a cabo las decisiones adoptadas en la fase de planificación.
- No es necesario que esta fase esté terminada para comenzar la fase de revisión.

## ④ Revisión

- El proceso de auditoría se debe revisar.
- Hay que asegurarse de las debilidades que se hayan detectado.
- Se debe informar de estas debilidades y de las mejoras necesarias para prevenirlas o eliminarlas.
- En muchas ocasiones estas debilidades no permiten alcanzar los objetivos de la auditoría, por lo que hay que pasar a la fase de corrección.

# Ciclo de vida

## ⑤ Corrección

- El programa de auditoría se debe ir mejorando teniendo en cuenta los resultados obtenidos en la fase de revisión.
- Esto supone volver a la fase de planificación para rediseñar los programas de trabajo y continuar el ciclo de auditoría.

## ⑥ Fin

- Cuando se han obtenido unos resultados adecuados se termina el trabajo y el ciclo se interrumpe.
- Tras la auditoría se organizan y archivan los documentos, de tal forma que se pueden reutilizar si es necesario.

# Planificación

- Las auditorías se deben planificar y supervisar para tener la seguridad de que los objetivos se alcanzan.
- En la planificación de la auditoría vamos a considerar 3 fases:
  - Planificación estratégica.
  - Planificación administrativa.
  - Planificación técnica.

# Planificación estratégica

- La planificación estratégica es una revisión global que permite conocer la empresa, el sistema y el control interno.
- El objetivo es hacer una primera evaluación de riesgos.
- Según los resultados de la evaluación se establecerán:
  - Los objetivos de la auditoría y su alcance.
  - Las pruebas que se deban aplicar.
  - El momento de realizar las pruebas.
- Para llevar a cabo esta tarea es necesario conocer:
  - Las características de los sistemas informáticos.
  - Los sistemas operativos.
  - Características de las bases de datos.
  - La organización de la empresa.
  - El sector donde opera la empresa.
  - La información comercial.

# Planificación estratégica

- La información puede obtenerse:

- ① Mediante entrevistas:

- Con los usuarios.
    - Con los proveedores de software y hardware.
    - Con los responsables del plan de contingencias.

- ② Inspeccionando documentación:

- Informes de auditorías anteriores.
    - Las normas y procedimientos de la empresa relacionados con la explotación.
    - Los planes de contingencias.
    - Agenda de trabajo.
    - Instrucciones sobre seguridad física y lógica.
    - Instrucciones sobre el encendido y apagado de equipos.
    - Contratos de mantenimiento con terceros.

# Planificación estratégica

- En función de la importancia de los riesgos que se hayan detectado, el auditor establecerá los objetivos de la auditoría.
- Estos objetivos permiten conocer el alcance de la misma.
- Se considera que el riesgo es la presentación negativa de un objetivo de auditoría.
- Si la oración negativa se transforma en oración afirmativa, se tiene como resultado un objetivo de control.

# Planificación estratégica

## Ejemplo

*Una de las preguntas típicas para una entrevista es “¿tiene su empresa normas escritas de cómo deben hacerse los trasvases de programas en desarrollo a programas en producción?”.*

*Si la respuesta es negativa, existe un riesgo por el hecho de que cada empleado podría hacer los trasvases sin tomar las medidas de seguridad necesarias y porque el proceso de trasvase no ha dejado pistas de auditoría para poder rehacer los pasos que se han dado y poder comprobar que el trabajo se ha realizado de manera correcta.*

*Sin embargo, el mero hecho de que no existan normas escritas no implica necesariamente que los trasvases se realicen mal. No obstante, como existe la posibilidad, lo convertimos en un riesgo de auditoría.*

# Planificación estratégica

## Ejemplo

*La debilidad sería la siguiente:*

*La empresa **no** tiene normas escritas de cómo deben hacerse los trasvases de programas en desarrollo a programas en producción.*

*El objetivo de control sería:*

*Comprobar que la empresa tiene normas escritas de cómo deben hacerse los trasvases de programas en desarrollo a programas en producción.*

- Para alcanzar los objetivos hay que diseñar una serie de pruebas.
- Cada una de estas pruebas es un procedimiento.
- Los procedimientos pueden basarse en métodos de verificación de cumplimiento o sustantivo, como veremos a continuación.



# Planificación estratégica

- Las **pruebas de cumplimiento** comprueban si las prácticas de la empresa se ajustan a los manuales.

## Ejemplo

*En el caso anterior no podemos realizar pruebas de cumplimiento porque el problema precisamente consiste en la no existencia de normas.*

- Las **pruebas sustantivas** consisten en revisar las aplicaciones concretas que se han desarrollado hasta ahora y comprobar si el riesgo se ha dado.

# Planificación estratégica

## Ejemplo

*En el ejemplo anterior podríamos revisar todas las aplicaciones que han pasado de desarrollo a explotación, si son pocas. En otro caso, elegiríamos un muestra representativa. Para estas aplicaciones revisaríamos que antes de pasarlas han sido sometidas a un lote de pruebas y las han superado satisfactoriamente. Las pruebas deben superar los requisitos y estándares del sector.*

## Discusión

*¿Qué tipo de aplicaciones elegirías para la muestra si hay demasiadas?*

# Planificación administrativa

- La planificación administrativa no se debe hacer hasta no haber terminado la estratégica.
- En esta fase deben quedar claros los siguientes aspectos:
  - Evidencia.** En este punto se puede hacer una relación con la documentación disponible de la etapa anterior, que se utilizará indicando el lugar donde se encuentra.
  - Personal.** De qué personal se va a disponer, qué conocimientos y experiencia es la ideal y si va a ser necesario o no contar con expertos.
  - Calendario.** Establecer la fecha de comienzo y finalización de la auditoría y determinar dónde se va a realizar cada tarea (en las dependencias del cliente o del auditor).
  - Coordinación y cooperación.** Es conveniente que el auditor mantenga buenas relaciones con el cliente, y que se establezca una buena cooperación sin dejar de cumplirse el principio de independencia.

# Planificación técnica

- En esta última fase se ha de elaborar el programa de trabajo.
- En la planificación estratégica se han establecido los objetivos.
- En la administrativa se han asignado los recursos.
- En la técnica se indican los procedimientos y las herramientas que se utilizarán para alcanzar los objetivos.
- El programa de auditoría debe ser flexible y abierto, de tal forma que se puedan ir introduciendo cambios.
- El programa y el resto de papeles de trabajo son propiedad del auditor.

# Planificación técnica

- El auditor no tiene obligación de mostrárselos al auditado (a no ser que sea el propio cliente), y debe custodiarlos el tiempo que marque la ley.
- La distribución ideal del tiempo empleado en realizar una auditoría sería:
  - Un tercio en planificar.
  - Un tercio en realizar el trabajo de campo.
  - Un tercio en hacer las revisiones y elaborar el informe.

# Procedimientos

- El objetivo general es asegurarse de que las funciones que sirven de apoyo a las Tecnologías de la Información se realizan con regularidad, de forma ordenada y satisfacen los requisitos empresariales.
- Para alcanzar el objetivo general se puede dividir en diversos objetivos específicos.
- Sobre estos objetivos se realizarán las pruebas oportunas para asegurarse de que el objetivo general se alcanza.

# Procedimientos

- El esquema de trabajo para cada uno de los objetivos específicos es el siguiente:
  - 1 Comprender las tareas del proceso que se está auditando.  
Si fuera necesario se amplían las entrevistas de la planificación estratégica.
  - 2 Determinar si son o no apropiados los controles que están instalados.  
Si fuera necesario se amplían las pruebas de la planificación estratégica.
  - 3 Hacer **pruebas de cumplimiento** para determinar si los controles que están instalados funcionan según lo establecido, de manera consistente y continua.

El objetivo de las pruebas de cumplimiento consiste en analizar el nivel de cumplimiento de las normas de control que tiene establecidas el cliente.

- 4 Hacer **pruebas sustantivas** para aquellos objetivos de control con los que no se haya podido quedar satisfecho con las pruebas de cumplimiento.

El objetivo de las pruebas sustantivas consiste en realizar las pruebas necesarias sobre los datos para que se proporcione la suficiente seguridad a la dirección sobre si se ha alcanzado su objetivo empresarial.

# Procedimientos

- Habrá que realizar el máximo de pruebas sustantivas si:
  - No existen instrumentos de medida de los controles.
  - Los instrumentos de medida que existen se considera que no son los adecuados.
  - Las pruebas de cumplimiento indican que los instrumentos de medida de los controles no se han aplicado de manera consistente y continua.
- El auditor debería haber realizado las suficientes pruebas sobre los resultados de las distintas tareas y actividades de la explotación del sistema como para concluir si los objetivos se han alcanzado.
- Con esa información se elabora un informe.



# Informes

- Una vez realizadas todas las fases anteriores, el auditor debe emitir un informe en el que exprese su opinión sobre el sistema auditado.
- Las opiniones pueden clasificarse por el tipo de trabajo y por los resultados del trabajo.
- Por el tipo de trabajo las opiniones se pueden expresar de forma positiva o negativa.
- Recordemos que la opinión positiva proporciona un nivel alto de seguridad, mientras la negativa proporciona un nivel moderado.

# La documentación y su organización

- La documentación de la auditoría es el registro del trabajo de auditoría realizado, y la prueba que sirve de soporte a las debilidades encontradas y a las conclusiones del auditor.
- Estos documentos se llaman genéricamente **papeles de trabajo**.
- Los papeles de trabajo se deben diseñar y organizar según las circunstancias y las necesidades del auditor.
- Han de ser completos, claros y concisos.

# La documentación y su organización

- El trabajo de auditoría debe quedar reflejado por los siguientes motivos:
  - Recogen la evidencia obtenida a lo largo del trabajo.
  - Ayudan al auditor en el desarrollo de su trabajo.
  - Ofrecen un soporte del trabajo realizado para poder utilizarlo en auditorías sucesivas.
  - Permiten que el trabajo pueda ser revisado por terceros.
- Una vez finalizada la auditoría, los papeles de trabajo son la única prueba que el auditor tiene de haber llevado a cabo un examen adecuado.
- Siempre cabe la posibilidad de que el auditor tenga que demostrar la calidad de su trabajo ante un tribunal.

# La documentación y su organización

- Los papeles de trabajo que el auditor va elaborando se pueden organizar en 2 archivos principales: el **archivo permanente** o continuo y el **archivo corriente** o de auditoría en curso.
- El archivo permanente contiene todos aquellos papeles que tienen interés continuo, como:
  - Características de los equipos y de las aplicaciones.
  - Manuales de los equipos y de las aplicaciones.
  - Descripción del control interno.
  - Organigramas de la empresa en general.
  - Consideraciones sobre el sector.
  - Escrituras y contratos.
  - En general toda aquella información que pueda tener importancia para auditorías posteriores.

# La documentación y su organización

- El archivo corriente se divide a su vez en **archivo general** y **archivo de áreas** o de procesos.
- En el archivo general se suelen archivar aquellos documentos que no tienen cabida específica en ninguna de las áreas del trabajo de auditoría:
  - El informe del auditor.
  - La planificación de la auditoría.
  - Los acontecimientos posteriores.
  - La correspondencia que se ha mantenido.
  - El tiempo dedicado por cada persona del equipo en cada proceso.

# La documentación y su organización

- El archivo por áreas mantiene un apartado para cada uno de las áreas en las que hemos dividido la auditoría.
- En cada apartado se guardan todos los documentos que hayamos necesitado para ese área.
- Hay 3 documentos imprescindibles en cada área:
  - Programa de auditoría para cada área.
  - Conclusiones del área.
  - Conclusiones del procedimiento.

# Auditoría de la explotación

- ① Introducción
- ② Aspectos legales
- ③ El informe de auditoría
- ④ Normas técnicas de auditoría
- ⑤ Auditoría de la explotación**
- ⑥ Auditoría de Internet
- ⑦ Auditoría de aplicaciones

# Auditoría de la explotación

- La auditoría de la explotación es el control que se realiza sobre las funciones del Sistema de Información para asegurar que las mismas se efectúen de forma regular, ordenada y que satisfagan los requisitos empresariales.
- Sus objetivos son:
  - Controlar los manuales de instrucciones y procedimientos de explotación.
  - Controlar los inicios de los procesos y otra documentación de funcionamiento.
  - Revisar la agenda de trabajo.
  - Verificar la continuidad del proceso.
  - Realizar controles sobre la explotación remota.
  - Comprobar que en ningún caso los operadores acceden a documentación que no sea la exclusiva para su explotación.
  - Revisar que existen procedimientos que impidan que puedan ejecutarse versiones de programas no activos.



# Auditoría de la explotación

- La competencia entre empresas obliga a obtener el máximo de los recursos disponibles.
- Uno de los recursos más importantes de cualquier empresa son los sistemas de información.
- Estos sistemas requieren de continuas actualizaciones para funcionar de manera óptima.
- La auditoría periódica es una forma de asegurar que estos sistemas son siempre los más adecuados.
- Detectar pronto las debilidades permite mejorar el sistema con el menor coste.

# Auditoría de la explotación

- Al hablar de sistemas de información nos referimos a:
  - Los datos.
  - Las aplicaciones.
  - La infraestructura.
  - El personal. En concreto, los conocimientos específicos que ha de tener el personal para planificar, organizar, administrar y gestionar el resto de datos.
- Para comprobar que el sistema funciona es necesario un sistema de control interno que prevenga los eventos no deseados, y que los detecte y corrija cuando ocurran.
- Es necesario recordar que si la auditoría se realiza solo parcialmente el resultado no se puede extrapolar a todo el sistema.

# Auditoría de Internet

- ① Introducción
- ② Aspectos legales
- ③ El informe de auditoría
- ④ Normas técnicas de auditoría
- ⑤ Auditoría de la explotación
- ⑥ Auditoría de Internet**
- ⑦ Auditoría de aplicaciones

# Auditoría de Internet

- La idea de “auditoría de Internet” es muy amplia y puede incluir factores muy diversos.
- Aquí nos centraremos en la privacidad y la protección de datos personales.
- La importancia de la introducción de mecanismos de control y revisión en este campo tiene cada vez más importancia.
- Todas las grandes empresas y la Administración Pública tienen presencia en Internet.
- No es solo cuestión de cantidad, además se ha pasado de dar algo de información a proporcionar servicios cada vez más complejos.

# Auditoría de Internet

- Un buen ejemplo es la posibilidad de tramitar por Internet la declaración de la renta.
- Estos servicios han supuesto un cambio en los “clientes”.
- Mientras que para obtener información los usuarios podían ser anónimos, para muchos servicios es necesario que se identifiquen.
- En el momento en el que se tratan datos confidenciales las compañías están sujetas al cumplimiento de ciertas normas.
- Su incumplimiento conlleva un serie de riesgos, tanto en términos económicos, debido a las posibles sanciones, como en pérdida de imagen y confianza.

# Auditoría de Internet

- Así pues, es necesario integrar la auditoría del cumplimiento de las normas de protección de datos en el ámbito de lo que constituye el canal de mayor exposición de una organización en su relación con las personas ajenas a la misma.
- Este control debe enfocarse desde 2 perspectivas: [legal](#) y [tecnológica](#).
- Ambos aspectos confluyen en la implantación de políticas de tratamiento de la información.
- La protección de datos se plasma en un conjunto de principios recogidos en la legislación vigente que es necesario conocer.
- Aunque parece simple, en muchas ocasiones es difícil cumplir la ley y cumplir los objetivos comerciales.

# Principios y derechos de protección de datos

- Empezaremos viendo qué son, formalmente, los **datos de carácter personal** y **el tratamiento de datos personales**.
- Siguiendo la definición de la Ley Orgánica de Protección de Datos (LOPD):

## Definición

*Se considera dato de carácter personal cualquier información concerniente a personas físicas identificadas o identificables.*

- Aunque el concepto de **identificada** está claro, es interesante clarificar el de **identificable**.

# Principios y derechos de protección de datos

- De nuevo según la LOPD:

## Definición

*... que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado.*

- Ahora nos encontramos con un término indeterminado “medios razonables”.



# Principios y derechos de protección de datos

- Este término debe ser interpretado por cada responsable y tener en cuenta que los mismos no solo hacen referencia a las posibilidades del responsable sino de otras personas.
- No obstante, es necesario poner de manifiesto que los criterios utilizados por las autoridades de control son bastante restrictivos.
- Habría que presentar evidencias serias y fundadas de que realmente los medios que habría que utilizar para identificar a la persona son realmente desproporcionados.
- No debemos olvidar que es un derecho fundamental de las personas que no puede ser evadido por mero interés económico.

# Principios y derechos de protección de datos

## Ejemplo

*La identificación del abonado que está detrás de la dirección IP que ha accedido a una determinada página web en ningún caso puede suponer un esfuerzo desproporcionado para el proveedor de acceso a Internet. Tiene registrado a quién corresponde la dirección IP en caso de asignación estática o, en caso de utilizar asignación dinámica, puede en todo momento conocer a quién se le asignó la misma en un cierto momento.*

# Principios y derechos de protección de datos

- En cuanto al concepto de **tratamiento de datos personales**, se definen como:

## Definición

*Las operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.*

# Encargo de tratamientos

- Un aspecto interesante en este campo son las subcontrataciones, como puede ser el **alojamiento web** (*webhosting*).
- También se subcontratan diversos servicios de recogida o tratamiento de datos, como la medición de audiencias.
- Esto se usa para modificar el perfil de la página.
- En estos casos es necesario un contrato con el suministrador del servicio en el que se detallan las tareas que va a realizar y las finalidades de las mismas.
- Se deben incluir, especialmente, las medidas de seguridad que va a adoptar, el compromiso de no utilizar los datos personales para ninguna otra finalidad y la devolución o destrucción de los mismos a la finalización del contrato.

# Encargo de tratamientos

- Parece ser que, aunque estas organizaciones firman continuamente contratos de servicio detallando varios aspectos, muchas veces estos contratos no contienen cláusulas sobre protección de datos.
- Esto se debe considerar como un riesgo, ya que cualquier autoridad puede investigar, bien de oficio o bien por una denuncia.
- Por ello, es aconsejable introducir cláusulas tipo en los modelos de contrato que se utilicen.
- Cada vez que se firme un nuevo contrato habrá que considerar si la cláusula estándar se adapta al servicio o, en caso contrario, modificarla adecuadamente.

# Legitimación de los tratamientos

- Un aspecto crucial del que depende el cumplimiento de las previsiones legales en materia de protección de datos es la **habilitación legal** para dicho tratamiento.
- En la legislación española el mecanismo primordial para que el tratamiento de datos sea legítimo es **contar con el consentimiento del cliente**.
- Este consentimiento es una manifestación de voluntad libre, específica, inequívoca e informada mediante la cual el interesado consiente el tratamiento de datos personales que le conciernen.
- El consentimiento no es el único mecanismo para legitimar el tratamiento de datos.

# Legitimación de los tratamientos

- Si existe una relación jurídica, comercial, laboral o contractual que implique la necesidad del tratamiento de datos, el tratamiento de los datos necesarios para cumplir con dicha relación es legítimo.
- Sin embargo, sigue siendo ilegal usarlos con otro fin o cederlos a terceros.
- Tampoco es necesario el consentimiento del interesado cuando los datos se recojan por parte de las Administraciones Públicas en el ejercicio de sus competencias.
- Esto significa que, en general, en el terreno de la Administración Electrónica no es necesario el consentimiento del afectado para el tratamiento de sus datos.
- Esto no significa que los puedan usar para cualquier finalidad.

# Legitimación de los tratamientos

- Por último, es legítimo usar los datos personales si el responsable está amparado por la ley.

## Ejemplo

*Las empresas están obligadas a dar los datos de sus trabajadores a la Seguridad Social.*

- Es importante recordar que el consentimiento debe ser explícito.



# Información al interesado

- Se establece:

## Definición

*Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*

- *De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.*
- *Del carácter obligatorio o facultativo de su respuesta a las preguntas que le sean planteadas.*
- *De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.*
- *De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.*
- *De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.*

# Información al interesado

- Por lo tanto, el deber de suministrar información a las personas cuyos datos se recogen a través de internet está descrita y puede ser comprobada por las autoridades.
- La legalidad del uso posterior depende de esta información.
- Esta información debe ser clara, comprensible y transparente.
- Si obtenemos información de una fuente pública (por ejemplo, para hacer publicidad) debemos indicar de dónde hemos sacado la información.

# Confidencialidad de la información

- En términos de Protección de Datos este principio se conoce como **Deber de Secreto**.
- Se refiere a la obligación del responsable del tratamiento y de cualquier otra persona que participe en el mismo de no revelar a nadie los datos personales que conozcan en el ejercicio de su actividad, incluso después de haber cesado en la misma o de haber cesado su relación con el responsable.
- Aunque al final el secreto depende de personas concretas el responsable debe tomar todas las medidas posibles para limitar los riesgos.
- En primer lugar, se deben definir las necesidades de información de cada persona en relación con la actividad que realiza.
- Cada persona solo debe acceder a la información estrictamente necesaria.

# Confidencialidad de la información

- En segundo lugar, se deben implementar procedimientos necesarios de identificación, autenticación y control de accesos.
- El control de los accesos no resulta fácil:
  - Por muchas medidas que pongamos no podemos garantizar la seguridad de los datos.
  - No siempre es fácil decidir cuál es el mínimo de información necesario para cada persona.
  - Ciertos empleados pueden ser reticentes a que se les limite la información.

# Confidencialidad de la información

- El riesgo de fuga de información se puede reducir mediante:
  - Formación.
  - Control.
  - Establecimiento de responsabilidades.
- La educación y formación de los trabajadores es indispensable.
- Es necesario concienciar sobre la confidencialidad de la información.
- Puede ser interesante que cada empleado firme un papel indicando que ha sido informado de sus obligaciones.

# Confidencialidad de la información

- Las herramientas de control dependen del tipo de organización.
- Siempre es útil establecer mecanismos de registro de los accesos a la información por parte de cada usuario.
- También puede ser necesario limitar la información que puede ser extraída (en formato físico o electrónico).
- Hay que valorar la importancia de los documentos frente a las incomodidades.
- Por último, hay que explicar las consecuencias de la divulgación ilícita de datos.
- Dichas consecuencias pueden ser desde sanciones internas a responsabilidades penales.

# Derechos de acceso, rectificación, cancelación y oposición

- Los usuarios tienen derecho a conocer la información que sobre ellos poseen los responsables que tratan sus datos.
- También tienen derecho a modificarla o cancelarla cuando sea incompleta o inexacta o su tratamiento no se ajuste a lo establecido.
- La ley española indica que estas modificaciones deben ser gratuitas.
- Cuando una persona ejerce estos derechos ante un responsable de tratamiento de datos, dicho responsable debe:
  - Concederle el derecho solicitado.
  - Denegarle el derecho. En tal caso, debe motivar la denegación y notificar que puede recurrir su decisión ante la autoridad de protección de datos competente.

# Derechos de acceso, rectificación, cancelación y oposición

- En el ámbito de Internet, hay 2 aspectos a resaltar respecto al ejercicio de estos derechos:
  - Hay que considerar la necesidad de asegurarse de la identidad del afectado cuando este ejerce sus derechos en línea.
  - Se debe permitir el ejercicio de estos derechos cuando los servicios se prestan en línea.
- Es decir, no importa cómo se proporcionan ni cómo se modifican los datos a la hora de ejercer estos derechos.
- Para identificarse se pueden usar firmas y certificados digitales.



# Derechos de acceso, rectificación, cancelación y oposición

- Sin embargo, ciertas operaciones que deberían usar este tipo de seguridad no la usan.

## Ejemplo

*El doble factor de autenticación no es obligado en entidades bancarias.*

- Sin embargo, es de esperar que la introducción del Documento Nacional de Identidad electrónico (e-DNI) sea cada vez mayor.
- Por último hay que considerar los plazos para hacer efectivos los derechos:
  - El de acceso debe contestarse en un máximo de un mes.
  - El resto en 10 días.

# Transferencias internacionales de datos personales

- Una transferencia internacional de datos es el envío de datos personales desde un país del Espacio Económico Europeo a otro país.
- Publicar los datos en una página web no se considera una transferencia de datos.
- Antes de hacer la transferencia es necesario saber si se considera un destino adecuado de protección de datos.
- Estos países son, según la AEPD, Suiza, Argentina, Canadá, Guernsey, Jersey, Isla de Man, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda, Japón, Reino Unido y Estados Unidos (solo para datos sobre pasajeros).
- En estos casos no es necesario adoptar ninguna medida.

# Transferencias internacionales de datos personales

- En otro caso, se debe estudiar si se puede llevar a cabo la transferencia si entra dentro de la ley:
  - Para solicitar ayuda judicial internacional.
  - Para asistencia sanitaria.
  - Para transferencias dinerarias con una legislación específica.
  - Por consentimiento explícito del interesado.
  - Si es necesario para salvaguardar el bien público.
- Si no podemos aplicar ninguna excepción, debemos solicitar a la AEPD una autorización.

# Comunicaciones comerciales no solicitadas (*spam*)

- Las comunicaciones comerciales no solicitadas, normalmente realizadas mediante correo electrónico, son uno de los aspectos más odiados de Internet.
- Estas comunicaciones se conocen como **spam**.
- El spam deteriora la imagen de una empresa.
- Además, si no se hace conforme a los requisitos legales, puede suponer sanciones.

# Comunicaciones comerciales no solicitadas (*spam*)

- Estas comunicaciones deben ser claramente identificables como tal.
- Deben indicar a la persona en nombre de la cual se llevan a cabo.
- Si se realizan por correo electrónico deben incluir al comienzo del mensaje la palabra “Publicidad”.
- Está prohibido enviar publicidad que no haya sido previamente autorizada o solicitada.

# Comunicaciones comerciales no solicitadas (*spam*)

- La norma dispone de un régimen más flexible en los casos en los que exista una relación contractual previa.
- Para ello es necesario que los datos de comunicación se hayan obtenido de forma lícita.
- Además, solo se pueden publicitar en esta caso productos similares a los que fueron objeto de contratación.
- Aun en este caso se debe ofrecer la posibilidad de oponerse mediante un procedimiento sencillo y gratuito.

# Comunicaciones comerciales no solicitadas (*spam*)

- Se establecen una serie de derechos de las personas que reciban estas comunicaciones, como el de revocar el consentimiento prestado.
- Debe ser suficiente con la simple notificación de su voluntad al remitente.
- Esta notificación debe ser posible realizarla de manera, de nuevo, sencilla y gratuita.
- La información sobre este proceso debe estar disponible de manera electrónica.

# Auditoría de aplicaciones

- ① Introducción
- ② Aspectos legales
- ③ El informe de auditoría
- ④ Normas técnicas de auditoría
- ⑤ Auditoría de la explotación
- ⑥ Auditoría de Internet
- ⑦ Auditoría de aplicaciones**



# Auditoría de aplicaciones

- La auditoría de aplicaciones busca que las aplicaciones funcionen correctamente y alcancen ciertos objetivos de calidad.
- Estas auditorías pueden cambiar la forma en que un proyecto o un producto se está gestionando.
- La auditoría de aplicaciones debe lograr:
  - El equipo de desarrollo se mentalice sobre el estado de su trabajo.
  - Se entiendan mejor las necesidades.
  - Proporcionar la oportunidad de expresar los problemas del desarrollo.

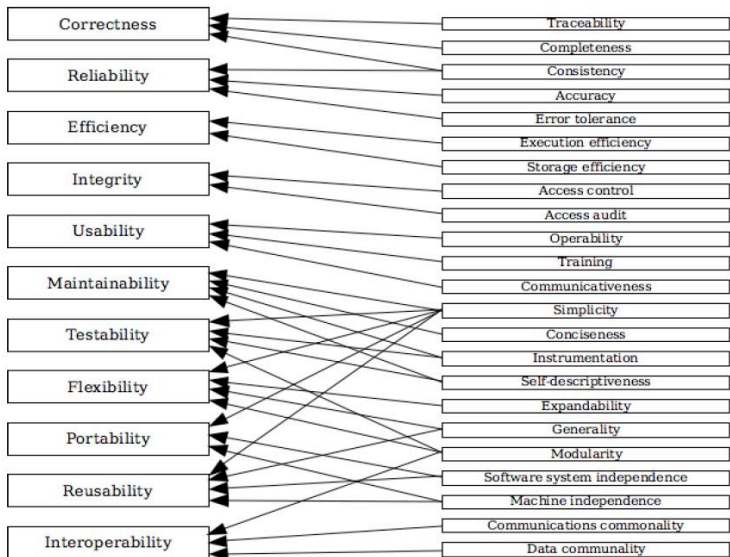
# Auditoría de aplicaciones

- El problema de las empresas a la hora de determinar la calidad es la complejidad de realizar el estudio del software.
- Esta complejidad se incrementa si el proceso por el cual se ha desarrollado el software es desconocido para los responsables de la auditoría.
- En este punto son útiles las métricas.
- Es mejor tener métodos automáticos para calcular las métricas, para hacerlas menos manipulables.

# Modelos de referencia

- Desde hace años existen modelos que descomponen la calidad en subcategorías para que se puedan calcular de manera sencilla.
- Un modelo muy utilizado utiliza los factores para calidad descritos en el tema anterior.
- Cada factor tiene asignadas distintas características que es necesario comprobar.
- Si todas las características asociadas a un factor se cumplen, entonces se cumplen los requisitos de calidad para dicho factor.

# Modelos de referencia: McCall



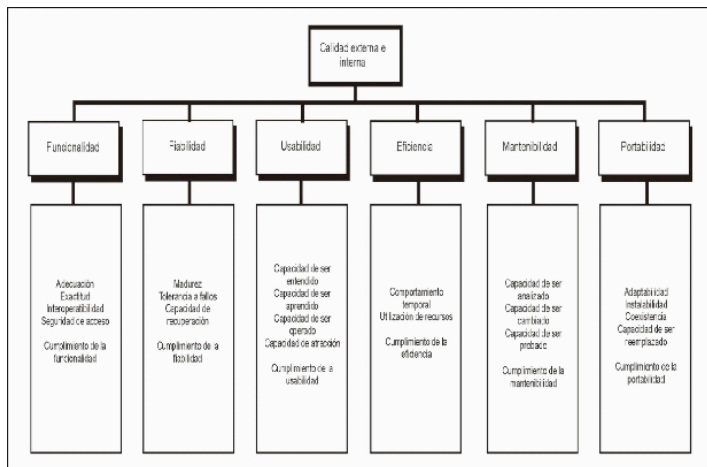
# Modelos de referencia

- En la calidad de una aplicación software se suelen distinguir 3 aspectos:
  - **La calidad interna.** Medible a partir de características intrínsecas, como el código fuente, etc.
  - **La calidad externa.** Medible en el comportamiento del producto, como, por ejemplo, en una prueba.
  - **La calidad en uso.** Medible durante la utilización efectiva por parte del usuario en un contexto determinado.

# Modelos de referencia

- Otro modelo importante es el que sigue la norma ISO 9126.
- Descompone la calidad jerárquicamente en una serie de características y sub-características.
- Se categorizan 6 características: funcionalidad, fiabilidad, usabilidad, eficiencia, mantenibilidad y portabilidad.
- La norma ISO 15598 da una visión del proceso de evaluación del software.
- Se usan métricas para los valores cuantificables.

# Modelos de referencia: ISO 9126



# Modelos de referencia: ISO 15598





# Modelos de referencia

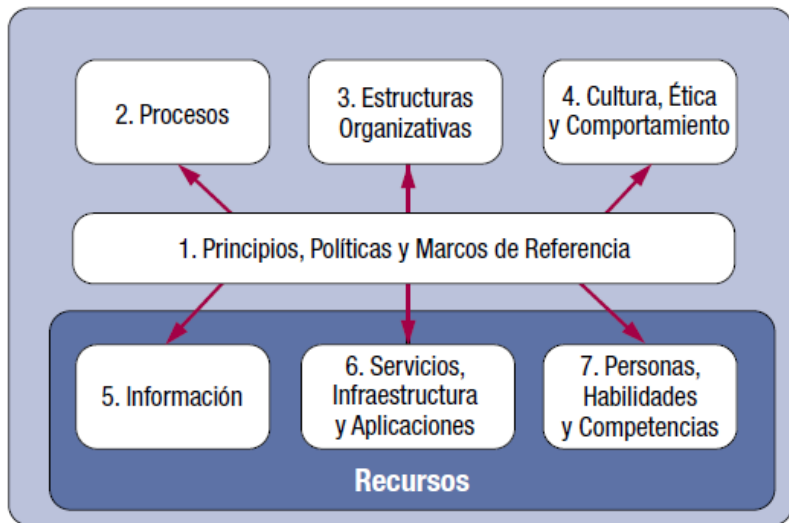
- Otro modelo de referencia es COBIT (Control Objectives for Information and Related Technology).
- Este modelo se estructura en 4 dominios de actividad:
  - Planificar y organizar.
  - Adquirir e implementar.
  - Entregar y dar soporte.
  - Monitorizar y evaluar.
- Al usar COBIT en auditoría debemos centrarnos en el último dominio: Monitorizar y evaluar.

# Modelos de referencia

- Este dominio tiene 4 subdominios:
  - Monitorizar y evaluar el rendimiento.
  - Monitorizar y evaluar el control interno.
  - Garantizar el cumplimiento legal y reglamentario.
  - Proporcionar controles.
- Incluso, el primer sub-dominio se divide en:
  - Enfoque de monitorización.
  - Definición y recopilación de la información.
  - Método de monitorización.
  - Evaluación del rendimiento.
  - Informes.
  - Acciones correctivas.

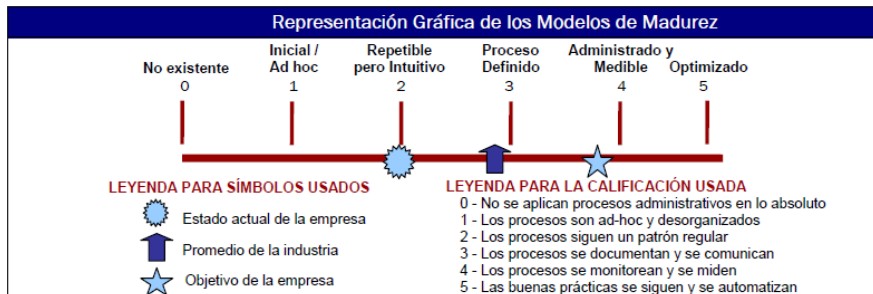
# Modelos de referencia

- En COBIT 5 se proporcionan ciertos facilitadores.



# Modelos de referencia

- Tras evaluar un modelo se puede determinar su “madurez”.



# Entornos para la evaluación de la calidad

- Recordemos que la medición es necesaria para auditar la calidad.
- Las métricas, revisiones e inspecciones deben:
  - ① Definir unos objetivos claros y medibles, determinando qué datos son necesarios y por qué.
  - ② Realizar las mediciones de manera periódica y frecuente, permitiendo tomar acciones correctivas en el momento oportuno.
  - ③ Automatizar el proceso de medición, ya que una medición manual puede hacer que no se muestre de manera clara y una muy costosa puede bajar su frecuencia.
  - ④ Definir diferentes niveles de abstracción, que eviten perderse en los detalles.

# Entornos para la evaluación de la calidad

- Existe un gran número de herramientas que permiten obtener mediciones y pruebas de una aplicación software.
- Estas herramientas de evaluación de la calidad se pueden dividir en 2 tipos:
  - **Herramientas de Análisis Dinámico.** Aquellas herramientas que realizan el análisis del software ejecutando el código.  
Estas herramientas suelen requerir el uso de bibliotecas especiales o pueden necesitar recompilar el programa.
  - **Herramientas de Análisis Estático.** Aquellas herramientas que llevan a cabo el análisis sin necesidad de ejecutar el código.  
Este tipo de análisis puede ser realizado sobre el código fuente o sobre el bytecode (o similar).
- En la actualidad existen varias herramientas de software libre para estas tareas.

# Fase 1 del plan de auditoría: plan de auditoría

- La primera tarea para obtener el plan de auditoría es definir el **alcance** y el **objetivo**.
- En una auditoría de aplicación puede haber muchas cosas a estudiar.
- Por ello es necesario concretar el objetivo.
- Conviene determinar:
  - La parte auditada.
  - El método.
  - Si será dinámico o estático.

# Fase 1 del plan de auditoría: plan de auditoría

- En una aplicación, a efectos de ser auditada, debemos destacar 2 elementos en su composición:
  - **Las fuentes**, es decir, las operaciones que el ordenador ejecuta y que pueden ser entendidas por una persona.
  - **Los objetos/ejecutables**, es decir, el programa en un lenguaje que pueda ser ejecutado.
- La calidad de las fuentes afecta al mantenimiento y a la escalabilidad.
- La falta de control sobre este punto hace que las aplicaciones no puedan mejorarse según va pasando el tiempo.



# Fase 1 del plan de auditoría: plan de auditoría

- Los ejecutables recogen el funcionamiento de la aplicación, formando la parte dinámica (ejecutable) de la misma.
- Las auditorías de ejecutables comprueban si el software se comporta de manera correcta según los requisitos.
- Recordando el ISO 9126, el objetivo de la auditoría es la funcionalidad, su fiabilidad, usabilidad, mantenibilidad, portabilidad o eficiencia.

## Fase 1 del plan de auditoría: plan de auditoría

- En cuanto al **método**, uno *dinámico* suele comprobar si la funcionalidad es la esperada o si la aplicación cumple los requisitos de carga o rendimiento.
- Para esta última comprobación se suelen utilizar cargas masivas de usuarios simulados.
- En los métodos estáticos se observan los productos que forman la aplicación (código, documentación y ficheros asociados, principalmente).
- En este caso se suele estudiar la calidad de la programación, el diseño y la mantenibilidad.

# Fase 1 del plan de auditoría: plan de auditoría

- Los estudios dinámicos suelen llamarse **pruebas**, mientras que a los estáticos se les denomina **inspecciones**.
- Una buena auditoría debe combinar métodos estáticos y dinámicos.

## Ejemplo

*Para comprobar la seguridad de una aplicación puede ser interesante comprobar que es segura intentado atacarla y, además, estudiar el código y el diseño para estudiar los métodos utilizados.*

# Fase 1 del plan de auditoría: plan de auditoría

## Discusión

*¿Para qué características es suficiente el análisis estático? ¿Y el dinámico?*

# Fase 1 del plan de auditoría: plan de auditoría

- El plan de auditoría debe **estimar y planificar los recursos**.
- Esta estimación permite elaborar el plan temporal y de recursos.
- También es necesario aprobar con el cliente la estructura de la auditoría.
- El cliente debe preparar la aplicación, reunir la documentación, etc.
- Además, el plan incluye la definición del **equipo de auditoría**, que puede contar con asesores externos.

# Fase 1 del plan de auditoría: plan de auditoría

- Por último, en el plan se definen las herramientas a ser utilizadas.
- Estas herramientas también se clasifican en estáticas y dinámicas.
- Entre las estáticas, se incluyen comprobaciones como:
  - Atributos privados no utilizados.
  - Variables locales no utilizadas.
  - Javadoc en clases e interfaces.
  - Evitar asignaciones en parámetros.
- Las herramientas dinámica incluyen comprobaciones sobre acceso en memoria (como las usadas en algunos compiladores de C++).

## Fase 2 del plan de auditoría: ejecución

- La ejecución supone llevar a cabo los objetivos y tareas, con las herramientas definidas, según el plan de la auditoría.
- Una de las actividades a realizar al comienzo de la auditoría es una reunión inicial.
- En esta reunión se presenta al equipo el cronograma y los objetivos del proyecto.
- Muchas de las tareas de comprensión y extracción de información se suelen organizar en torno a reuniones de revisión.

## Fase 2 del plan de auditoría: ejecución

- En estas reuniones se examina la aplicación detectando e identificando anomalías, con el objetivo de:
  - Verificar que la aplicación satisface una serie de atributos específicos de calidad.
  - Verificar que la aplicación es conforme a las normativas, estándares, directrices, planes y procedimientos aplicables.
  - Identificar las desviaciones respecto de los estándares y las especificaciones.
  - Recoger datos sobre las aplicaciones.
- En las reuniones se suele trabajar con los ficheros fuente, la aplicación en ejecución o con productos intermedios, dependiendo de las características estudiadas.



## Fase 3 del plan de auditoría: análisis, síntesis y presentación de resultados

- El auditor debe elaborar una serie de comentarios en los que se describa la situación, el riesgo existente, la deficiencia a solucionar y, en su caso, la posible solución.
- La presentación de los datos y los informes asociados deben estar preparados para el nivel de abstracción que requerirán los lectores del mismo.
- Suele haber 2 tipos de lectores:
  - **Directivos**, para los que se suelen presentar informes resumen con un nivel de abstracción alto.
  - **Desarrolladores**, para los que se preparan informes con mayor detalle.

## Fase 3 del plan de auditoría: análisis, síntesis y presentación de resultados

- En el caso de informes a directivos los hallazgos encontrados en la auditoría suelen resumirse y agruparse.
- Los hallazgos pueden acompañarse del lugar en que se han encontrado.
- También se puede añadir otra información para tomar decisiones posteriores.
- Esta información incluye la severidad del problema, una estimación del coste de arreglarlo y su prioridad.
- Los informes deben ser concisos.
- Una vez elaborados los informes son comentados y discutidos con los responsables de las áreas afectadas.
- Tras esta reunión, se presenta el informe final.

# Recomendaciones y buenas prácticas

- Utilizar métricas y factores cuantitativos.
- La frecuencia de las auditorías depende de su complejidad. Por ello, automatizar las métricas de aplicaciones complejas es esencial.
- Sin embargo, debe evitarse recopilar demasiada información. Para ello, deben estar claros los objetivos de la auditoría.
- En cada auditoría es importante definir qué información mostrar, cuándo y a quién. Esto hace que existan en general varios informes finales.
- Puede ser conveniente subcontratar la auditoría. De esta manera se obtiene más objetividad y probablemente se reducen los costes.