



Introducción a la Auditoría Informática

Barcelona, 16 de febrero de 2006



18:30 – 21:30

2 sesiones con descanso

Aspectos generales de la Auditoría de seguridad

- Introducción a la Auditoría Informática
- Metodología

→ **Enfoques CISA
y COBIT**

Algunos trabajos

- Auditoría de Seguridad informática
 - Plataforma Internet
 - Seguridad física
 - Aplicaciones Web
- Auditoría de los requerimientos de seguridad estándares en el tratamiento de los PIN
- Auditoría del Reglamento de Medidas de Seguridad de la LOPD
- Sistema de alarmas automatizado

**Requerimientos
y normativa
externa**

Introducción a la Auditoría Informática

- **Índice**

- Definición
- Enfoque tradicional y nuevo enfoque
- Necesidad de la Auditoría Informática
- Misión de la Auditoría Informática
- Objetivos de la Auditoría Informática
- Implicaciones de la Auditoría Informática
- Funciones de Auditoría Informática y del Auditor Informático
- Riesgo
- Control Interno

Definición

*“Auditoría Informática es el **proceso de recoger, 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”*

Ron Weber Profesor de Sistemas de Información en la Escuela de Comercio y Director de Investigación en la Facultad de Negocios, Económicas y Leyes de la Universidad de Queensland

- **Enfoque tradicional: Complemento a la Auditoría Financiera**
 - ¿Auditoría con ordenador - Apoyo informático a la auditoría - Auditoría informática...?
 - Orientada a la inspección y fiscalización de los sistemas
 - Planificación de la auditoría informática con el área de finanzas
 - Métodos y herramientas tradicionales y limitados
 - Recursos humanos con escasa formación técnica informática
 - Percepción del resto de la Organización:
 - Inspección
 - aporta poco valor añadido
 - trabajo adicional para el auditado

- **Nuevo enfoque: Auditoría de Sistemas de Información**

- El Departamento de Auditoría de SSII es una unidad de soporte más de la organización, que presta servicios de control, de alto valor añadido para el resto de unidades de negocio y de soporte (incluidos otros departamentos de auditoría)
- La planificación del servicio de auditoría de sistemas se realiza involucrando a las unidades de negocio y de soporte
- Utiliza métodos y herramientas actualizados
- Recursos humanos altamente especializados (internos / externos)
- Percepción del resto de la Organización:
 - Búsqueda de la participación de los auditores
 - Recomendaciones de alto valor añadido para los intereses del negocio

- **Necesidad de la auditoría informática**

- Los procesos de negocio se basan fuertemente en los sistemas de información
- Se toman decisiones estratégicas basadas en la información extraída de los sistemas de información
- Posibilidad de fraude o malversación si no se controlan los sistemas informáticos
- Grandes inversiones en recursos informáticos: hardware, software y personal técnico
- Necesidad legal de mantener la intimidad de las personas. (RD994/1999 de LOPD)
- Se manejan grandes volúmenes de datos

- **Misión de la Auditoría de SSII**

- Convertirse en la referencia de la Dirección de la Compañía, así como de las Unidades de negocio y soporte, en relación al control, la integridad, confidencialidad y disponibilidad de los sistemas de información
- Ser el proveedor de recomendaciones de control de alto valor añadido para el negocio
- Especialmente en aquellas áreas que puedan mitigar riesgos de índole económico, adaptar los controles al marco legal vigente y a la normativa establecida o garantizar la integridad de la información enviada a clientes y entidades oficiales a las que se reporta

- **Objetivos de Auditoría de SSII**

- Auditoría de Sistemas de Información es una función que está al servicio de las áreas de negocio y de apoyo y que tiene como objetivos los siguientes:
 - Revisar la existencia y suficiencia de controles de los sistemas de información que soportan los procesos de negocio
 - Validar que los procesos informáticos recogen fielmente la estrategia y operativa de negocio, así como la normativa del sector
 - Evaluar la eficacia y eficiencia del uso de los recursos informáticos
 - Analizar permanentemente los riesgos para el negocio derivados de la tecnología
 - Mentalizar al resto de unidades de los riesgos y amenazas que se derivan de la utilización indebida de los sistemas de información

- **Implicaciones de la auditoría informática:**
 - Evaluación
 - Emisión de opinión objetiva e independiente.
 - Emisión de recomendaciones sobre la fiabilidad de un sistema informático.

- **Funciones** de Auditoría de SSII:
 - Evaluar de forma continua los riesgos asociados a los sistemas actuales y proponer mejoras en los controles existentes o controles adicionales
 - Asesorar en los riesgos asociados a la tecnología que soportará las nuevas iniciativas de negocio y proponer soluciones para mitigar los posibles riesgos
 - Evaluar la eficacia y eficiencia del uso de los recursos informáticos de la organización, asegurando su salvaguarda y vigilando el cumplimiento del marco legal establecido
 - Revisar el grado de implantación de los proyectos realizados en el marco del plan de sistemas y el plan de seguridad de la información
 - Prestar soporte informático a las iniciativas de auditoría financiera, a través de herramientas informáticas (CDAA) o de formación

- **Funciones del auditor informático:**

- Participar en las revisiones desde la fase de diseño hasta la implantación y mantenimiento de las aplicaciones informáticas y en las fases de realización de cambios importantes.
- Revisar y evaluar los controles implantados en los sistemas informáticos (verificar su adecuación).
- Revisar y evaluar el nivel eficacia, utilidad, fiabilidad y seguridad de los equipos e información.

- **Riesgo**

- "El potencial de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y ocasione la pérdida o daño de los mismos. El impacto o severidad relativos al riesgo es proporcional al valor de la pérdida o daño y a la frecuencia estimada de la amenaza para el negocio"
- Un riesgo es una situación de peligro no deseada por parte de una Entidad en su operativa diaria.

- **Riesgo Informático**

- Es el peligro de que alguno de los componentes de una instalación informática (bien sean activos, bien software o datos) sufra alguna pérdida, omisión o situación anómala.

- **Control interno: mitiga el riesgo hasta un nivel aceptable**

- “Cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos”
- Controla que todas las actividades del sistema informático sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la Dirección.
- Suele ser un staff de la Dirección del Departamento de Informática.

- **Objetivos del control interno**

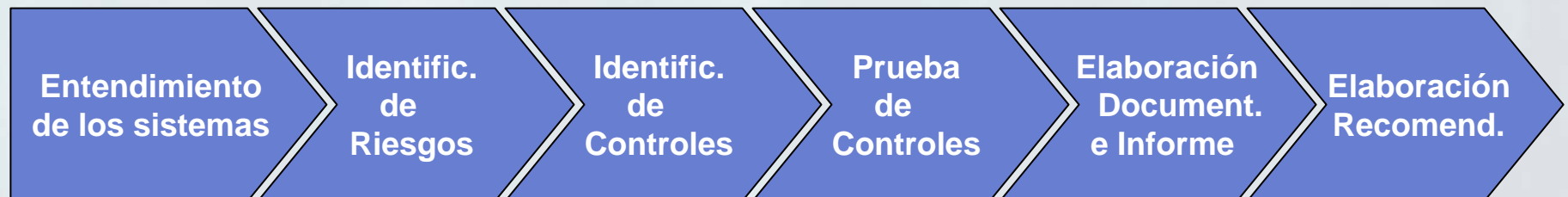
- Controlar que todas las actividades se realizan cumpliendo con los procedimientos y normas fijados.
- Asesorar sobre el conocimiento de las normas.
- Colaborar y apoyar el trabajo de la Auditoría Informática (externa o interna).
- Definir, implantar y ejecutar mecanismos y controles para comprobar los logros del servicio informático.

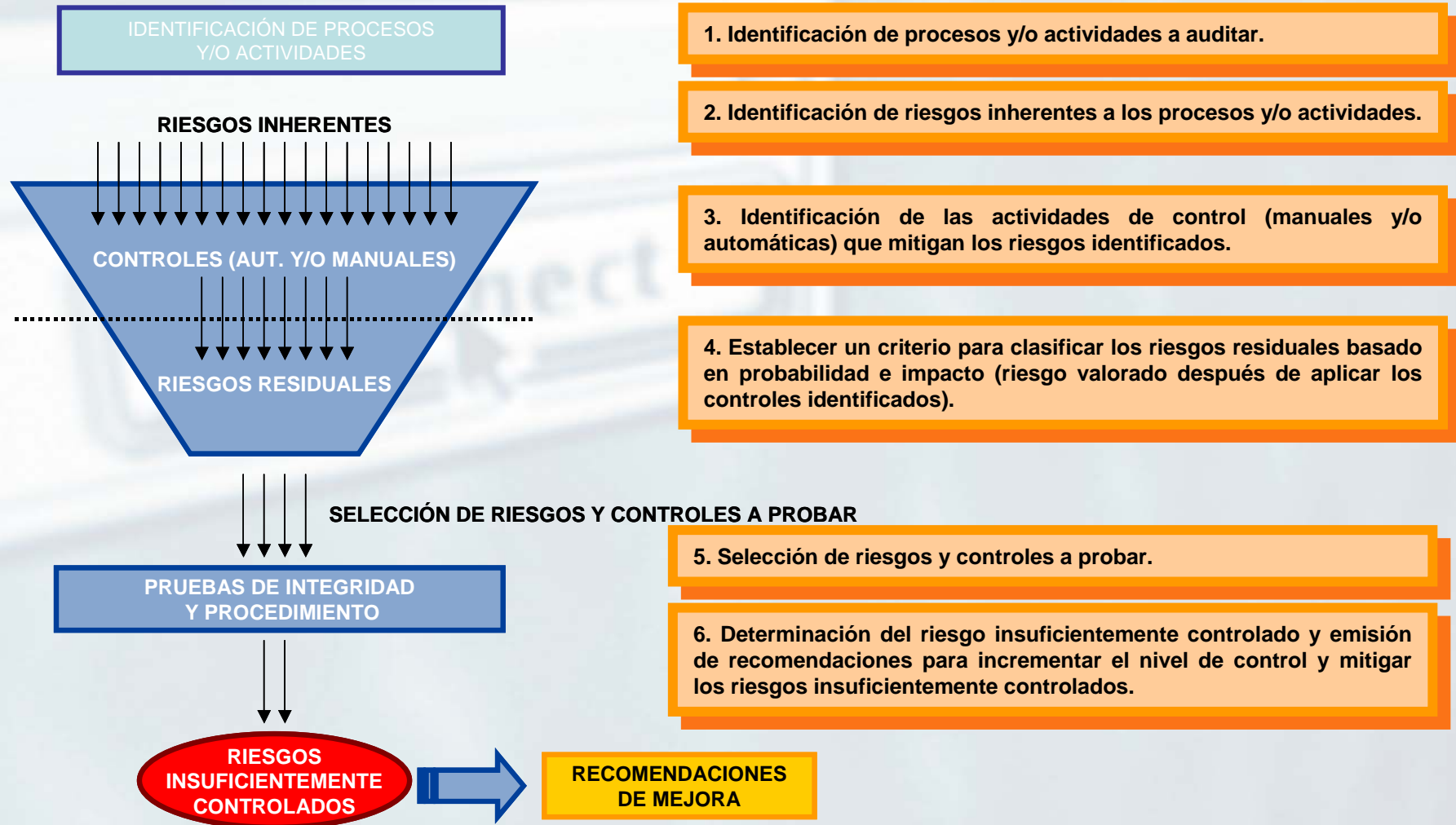
Ejemplos de Auditorías Informáticas



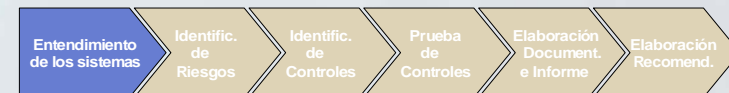
Metodología de la auditoría informática

- **Índice:**
 - Entendimiento de los sistemas
 - Identificación de los riesgos
 - Identificación de controles
 - Tipos de controles
 - Pruebas de los controles
 - Elaborar la documentación
 - Conclusión de la auditoría
 - Elaboración de las recomendaciones



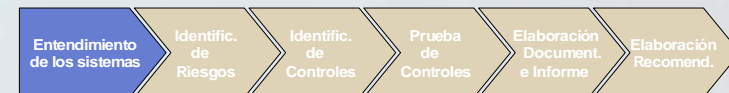


- Solicitud de una descripción general de los Sistemas:
 - Tipos y ubicaciones importantes de los ordenadores centrales del sistema de información
 - Para cada ubicación de procesamiento:
 - Identificar sistemas relevantes
 - Naturaleza general de la organización por su función de procesamiento
 - Tipo de actividades realizadas (operaciones del ordenador, desarrollo y mantenimiento de sistemas, etc.)
 - Programas informáticos utilizados
 - Gestión del ambiente de control y extensión y políticas comunes a las distintas ubicaciones
 - Identificar como interactúan los ordenadores de la organización, LAN o WAN



- **Para cada sistema de aplicación a auditar se deben identificar los siguientes aspectos:**

- Nombre de la aplicación
- Fecha de implantación
- Desarrollo interno/externo
- Paquete estándar
- Suministrador
- Año de compra
- Lenguajes de programación
- Batch / On-Line
- Usuarios principales
- Breve descripción de la aplicación
- Organigrama / flujograma
- Datos de entrada
- Descripción
- Volumen
- Frecuencia
- Dispositivo
- Ficheros / Bases de datos
- Estructura
- Volumen de registros
- Maestro / Temporal
- Procesos
 - Tipos de cálculos.
 - Tipo de transacciones (a/b/m, consulta)
- Salidas
 - Tipo (impresos, informes, documentos, ficheros)
 - Frecuencia
 - Distribución
 - Interfases con otros sistemas
- Seguridad: controles de acceso
- Explotación
 - Cadenas de Control
 - Versiones de los ficheros
 - Número y frecuencia de backups
 - Disposiciones para caso de errores
 - Tipos de problemas experimentados
- Documentación existente



- Una vez entendida, a alto nivel, la situación actual de los sistemas de información del cliente, es necesario centrarse en la **identificación de riesgos potenciales** que puedan afectar a los sistemas.



Auditoría de controles generales de Sistemas de información



- **Auditoría de controles generales de Sistemas de información**
- Riesgos en la estrategia y planificación de los sistemas de información:
 - Falta de planificación y responsables para la toma de decisiones
 - Falta de presupuestos para la gestión de los recursos informáticos
 - Falta de objetivos a corto y medio plazo, o que estos no se correspondan con los objetivos estratégicos de la empresa
- Riesgos típicos en políticas, normas y procedimientos:
 - Falta de estándares en forma de políticas, normas o procedimientos para la gestión de los recursos informáticos
 - Segregación de funciones en puestos clave para la toma de decisiones
- Riesgos relacionados con la seguridad de la información:
 - Falta de una política de seguridad
 - Acceso lógico a los sistemas
 - Registro y supervisión de los accesos al sistema (ficheros de log)
 - Acceso a las ubicaciones de los ordenadores centrales, controles ambientales implantados, supervisión de los mismos, etc.



- **Auditoría de controles generales de Sistemas de información**
- Riesgos típicos relacionados con la política de continuidad y de recuperación:
 - Imposibilidad de continuar las operaciones de los sistemas y del negocio, tras la ocurrencia de un desastre
 - No poder recuperar la información perdida
- Riesgos del área de desarrollo, adquisición y mantenimiento de sistemas:
 - Documentación de desarrollo de programas
 - Segregación de funciones entre los entornos de desarrollo, preproducción (si existe) y producción
 - Controles en el paso a producción de los programas en desarrollo
 - Entradas y salidas de datos
- Riesgos del área de Operaciones – Explotación de sistemas pueden ser:
 - Falta de procedimientos de planificación y supervisión de las actividades en producción
 - Segregación de funciones entre los entornos de producción y desarrollo
 - Falta de documentación relativa a las aplicaciones en producción (desconocimiento o concentración de saber en un único punto)



- **Auditoría de controles generales de Sistemas de información**
- Principales riesgos relacionados con las telecomunicaciones:
 - Nivel de seguridad en los accesos entre redes y más cuando se realizan con redes externas como Internet
 - Uso del correo electrónico, que cada vez da mayores quebraderos de cabeza a los administradores de redes
 - Falta de estrategia de comunicaciones, que puede ocasionar pérdidas económicas, de información y de imagen
- Riesgos relacionados con el área de microinformática:
 - Instalación de programas sin licencia de uso
 - Pérdida de información en los ordenadores clientes (copias de seguridad)
 - Uso de los ordenadores para otros fines distintos a la actividad del usuario



- **Una vez identificados los riesgos, habrá que proceder a identificar los controles utilizados por la entidad y posteriormente decidir si se adopta una estrategia de confianza en los controles o se realizan pruebas sustantivas:**
 - Proceder a la identificación de los distintos tipos de controles
 - También evaluamos el ambiente de control para determinar si los sistemas de información son adecuados
 - Los controles que queremos identificar y probar son aquellos que son efectivos y relevantes al trabajo de auditoría, y que pueden ser probados de una manera eficiente
 - Los controles efectivos son aquellos que previenen o detectan irregularidades y errores importantes en los sistemas.



- **CONTROLES INFORMÁTICOS:**

- *“Son mecanismos que tratan de asegurar que el desarrollo, puesta en marcha, operación y mantenimiento de los sistemas de información en una Organización se comporten de una manera planificada y controlada”.*
- *“Un control es una medida establecida para tratar de impedir, detectar o corregir una situación no deseada, anómala, o incorrecta, en definitiva, un riesgo”.*



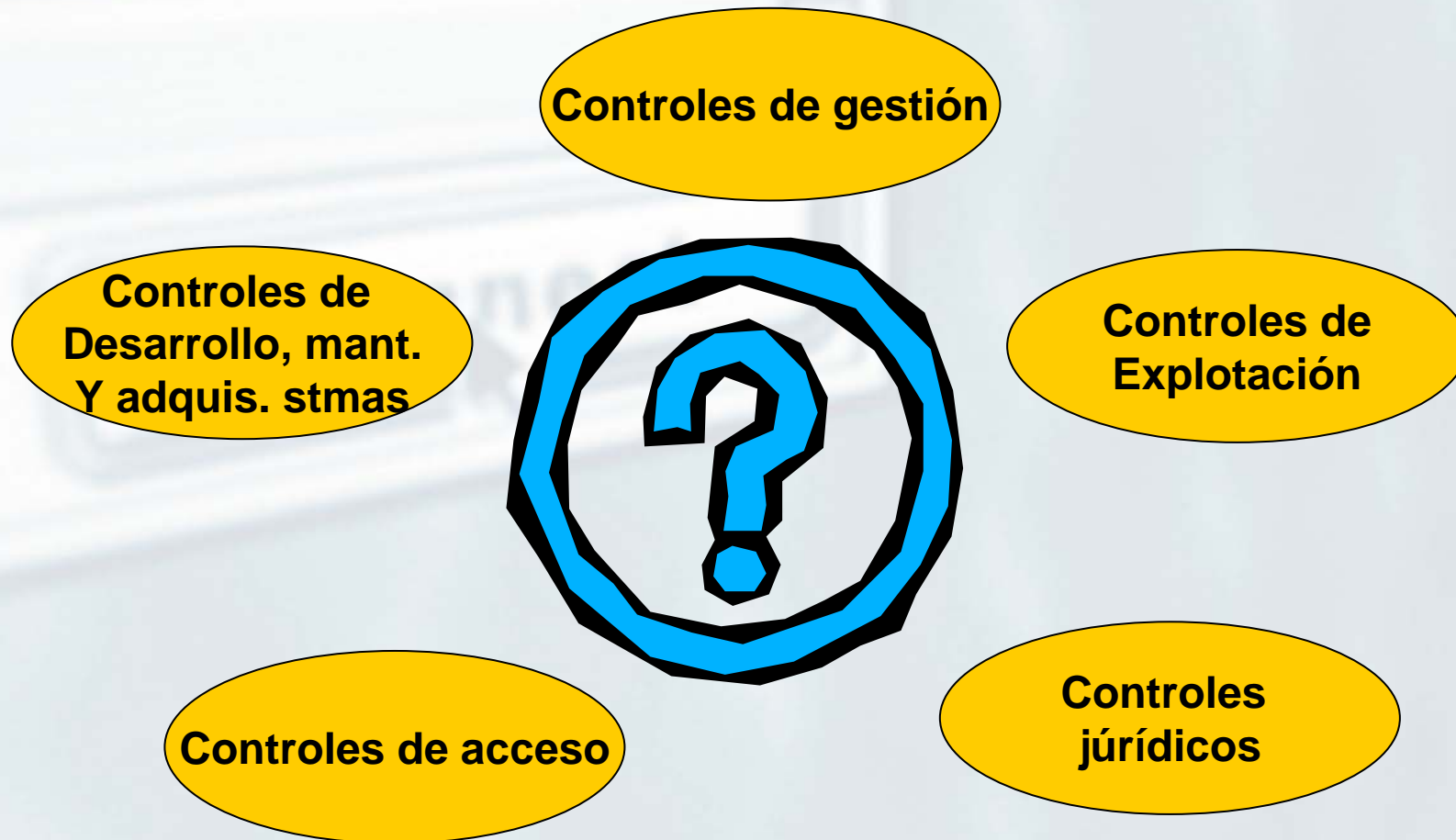
- **Clasificación de controles**
- Por su alcance:
 - Generales
 - De aplicación
- Por su ejecución en el tiempo:
 - Preventivos
 - Detectivos
 - Correctivos
- Por su implementación:
 - Automáticos
 - Manuales
- Otros tipos:
 - De integridad, existencia, exactitud, etc.



- Según el alcance:
 - Los **controles generales** son aquellos que están relacionados con todas las actividades del entorno informático. En definitiva afectan a todos los datos y procesos informáticos de una Organización.
 - Los **controles de aplicación** son aquellos relacionados con las aplicaciones informáticas individuales (integrados dentro de los sistemas de información centrados alrededor de dichas aplicaciones).



Auditoría de controles generales de Sistemas de información



- **Controles Generales:** Controles de Gestión:
 - Planificación del Departamento de Informática: planes a corto y largo plazo consensuados con los planes generales de la organización.
 - Políticas, estándares y procedimientos: base para la planificación, control y evaluación por la dirección de las actividades del Departamento de Informática.
 - Responsabilidades organizativas y gestión del personal: ubicación del Depto. de Informática, descripción de responsabilidades dentro del Depto. de Informática, segregación de funciones, descripción de puestos, gestión del personal, formación del personal.
 - Garantía de Calidad del Departamento de Informática: responsables de Calidad, aspectos organizativos, plan de revisión de la garantía de Calidad .
 - La función de Auditoría Interna: plan de auditoría, competencia técnica, formación continuada, independencia, revisiones e informes.



- **Controles Generales:** Controles de Desarrollo, Adquisición y Mantenimiento de Sistemas:
 - Revisión de los procedimientos para la adquisición de sistemas
 - Revisión de las metodologías utilizadas para el desarrollo y mantenimiento de sistemas:
 - Controles del ciclo de vida del desarrollo de sistemas (análisis, diseño, desarrollo, pruebas, implantación, producción y mantenimiento)
 - Segregación de funciones (desarrollo, pruebas y explotación)



- **Controles Generales:** Controles de Acceso:
 - Seguridad Física, revisión de los elementos de control establecidos para preservar la seguridad en los accesos a la sala de los ordenadores centrales (CPD):
 - Controles de acceso (llaves, tarjetas magnéticas, códigos de acceso)
 - Controles medioambientales (falso suelo, refrigeración, sistemas antiincendios, habitabilidad, sistemas de alimentación ininterrumpida)
 - Política de Seguridad, analizar los procedimientos de seguridad:
 - Objetivos de seguridad
 - Alcance de la política
 - Responsabilidades y papeles asignados
 - Seguridad Lógica, revisión de los procedimientos de seguridad lógica establecidos (Política de Seguridad):
 - Identificación de usuarios
 - Políticas de contraseñas



- **Controles Generales:** Controles de Explotación de Sistemas de Información (Operaciones):
 - Revisión de los procedimientos establecidos en el área de explotación, producción u operaciones: segregación de funciones, sistemas de planificación de procesos (batch, on line, carga de trabajo), integridad y exactitud de la información, gestión de problemas, gestión de cambios, sistemas de almacenamiento de datos, control y distribución de las salidas (listados)
 - Revisión del Sistema Operativo: selección, instalación, mantenimiento, control de cambios, gestión de problemas, seguridad lógica
 - Planificación ante contingencias: plan de recuperación de desastres



- **Controles Generales:** Controles Jurídicos:

- Su función es comprobar que la utilización de la Informática se ajusta a la legislación vigente (LOPD, Ley Orgánica de Protección de Datos de Carácter Personal)
- Medida preventiva contra sanciones administrativas o penales
- Ámbitos de control a tener en cuenta:
 - Los programas y el soporte físico: comprobación de los contratos de hardware, control de las licencias de uso de las aplicaciones, elaboración de trabajos auxiliares, contratos de entrada de datos, subcontratación de la gestión de algunos sectores de la empresa
 - Las personas: accesos a la información atendiendo a la “sensibilidad” de la misma, conocimiento de la normativa y mantenimiento de una actitud ética con los ficheros, descripción en los contratos laborales de sus funciones y responsabilidades
 - Los ficheros: niveles de protección, seguridad del fichero, responsable del fichero

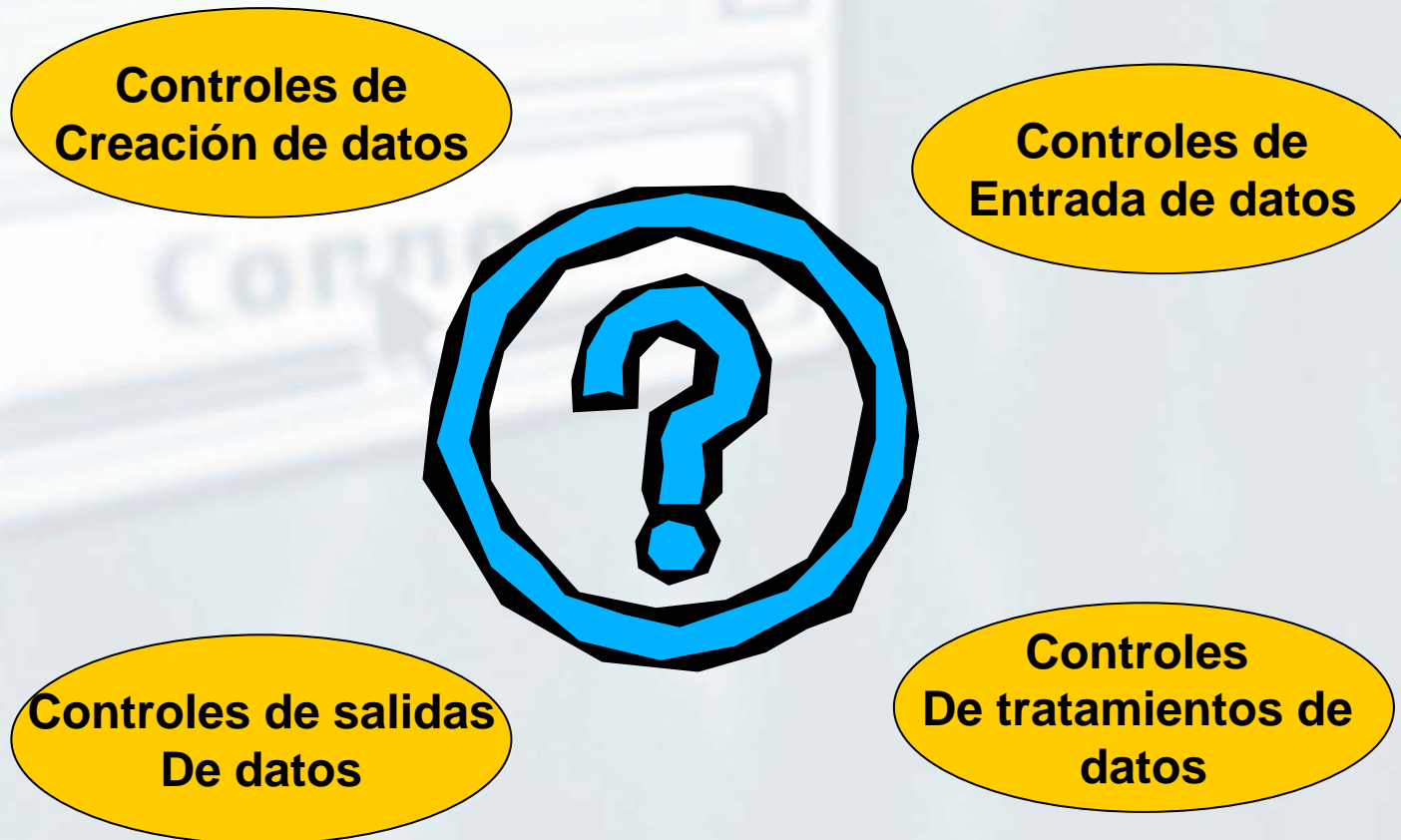


- **Controles de Aplicaciones**

- Auditoría de una aplicación: *“Revisión de la eficacia del funcionamiento de los controles diseñados para cada uno de los pasos de la misma frente a los riesgos que tratan de eliminar o minimizar”*.
- Tipos de controles a tener en cuenta:
 - Controles de Creación de Datos
 - Controles de Entrada de Datos
 - Controles de Tratamientos de Datos
 - Controles de Salidas de Datos



Controles de aplicaciones



- **Controles de Aplicaciones:** Controles de Creación de Datos:
 - Procedimientos de preparación de los datos
 - Diseño de documentos fuente
 - Control de documentos fuente
 - Autorización de entrada de datos
 - Retención de documentos fuente
- **Controles de Aplicaciones:** Controles de Entrada de Datos:
 - Conversión y entrada de datos
 - Validación y corrección de datos



- **Controles de Aplicaciones:** Controles de Tratamientos de Datos:
 - Integridad en el tratamiento de los datos
 - Validación y corrección del tratamiento de los datos
 - Gestión de errores en el procesamiento de los datos
- **Controles de Aplicaciones:** Controles de Salida de Datos:
 - Revisión de la salida
 - Cuadre y reconciliación de la salida
 - Distribución de salidas
 - Gestión de errores en la salida
 - Seguridad sobre las salidas



- Por su ejecución en el tiempo:
- **Controles Preventivos**
 - Son los destinados a evitar que los riesgos se materialicen. En informática, son los más cercanos al origen del dato.
- **Controles Detectivos**
 - Identifican los errores cuando ya han ocurrido. Asociados a las llamadas pistas de auditoría
 - Ejemplo: Programa de validación del valor de un número dentro de un rango prefijado.
- **Controles Correctivos**
 - Eliminan o reducen los efectos de los errores identificados.
 - Ejemplo: Software de comunicaciones que solicita la retransmisión de los datos si los recibe incompletos.



- Por su implementación:
- Automáticos
 - Programados en las mismas aplicaciones informáticas o en la secuencia de ejecución de dichas aplicaciones.
 - Ejemplo: proceso de validación de datos de entrada; en una cadena de aplicaciones, validación de que una aplicación ha finalizado antes de empezar la siguiente.
- Manuales o de usuario
 - Los que se realizan con la información que la aplicación suministra.
 - Ejemplo: listados de cuadros totales.



- Otros tipos de controles:
- **Controles de autenticidad**
 - Destinados a verificar la identidad del individuo o proceso que quiere realizar alguna acción sobre el sistema.
 - Ejemplos: “passwords”, PIN’s para cajeros automáticos, firmas digitales.
- **Controles de exactitud**
 - Instaurados para asegurar la corrección de los datos y los procesos en un sistema.
 - Ejemplos: validación por programa informático del NIF, del dígito de control bancario, de que un campo numérico contiene únicamente datos numéricos, etc.



- Otros tipos de controles (cont.):
- Controles de integridad
 - Tienden a asegurar que no faltan datos y que todos los procesos se llevan a su conclusión correcta hasta el final de los mismos.
 - Ejemplo: Validación por programa informático de que se rellenan todos los campos de entrada de datos; registros de ficheros informáticos numerados
- Controles de redundancia
 - Tienden a asegurar que los datos se procesan sólo el número de veces para el que han sido definidos.
 - Ejemplo: contadores en los programas informáticos



- Otros tipos de controles (cont.):
- Controles de privacidad
 - Tienden a asegurar que los datos están protegidos frente a su revelación accidental o no autorizada:
 - Ejemplo: passwords, diario de registro de los accesos al sistema informático, cifrado de datos.
- Controles de disponibilidad
 - Tienden a asegurar la disponibilidad permanente de todos los recursos del sistema.
 - Ejemplo: mantenimiento preventivo, diarios de actividad del sistema, backups de los ficheros de datos



- Otros tipos de controles (cont.):
- Controles de eficiencia y eficacia
 - Tienden a asegurar que el sistema usa el mínimo de recursos para realizar sus tareas y que todos funcionan eficazmente.
 - Ejemplo: estudios de rendimiento del sistema, diario de utilización de recursos informáticos.
- Controles de pista de auditoría
 - Para asegurar que existe un registro cronológico de todos los sucesos ocurridos en un sistema. Son básicamente dos:
 - De operaciones: el uso y consumo de los recursos de un sistema.
 - De datos: muestra el origen y la naturaleza de los datos y procesos que actualizan las bases de datos y ficheros.



Prueba de los controles

- Permiten obtener evidencia y verificar la consistencia de los controles existentes y también medir el riesgo por deficiencia de estos o por su ausencia.
- Toda opinión o evaluación de un auditor debe estar basada en pruebas realizadas y en la evidencia obtenida de acuerdo a una normativa profesional.
- El alcance de las pruebas es verificar el nivel de cumplimiento de los controles establecidos



Prueba de los controles

- DESCRIPCIÓN DE PRUEBAS HABITUALES
 - Organización y Dirección
 - Examinar el proceso de planificación de sistemas de información.
 - Lectura de actas de sesiones del Comité de Informática dedicadas a la planificación estratégica.
 - Lectura y comprensión del Plan Informático.
 - Realización de entrevistas con el Director de Informática.
 - Seguridad Física
 - Observación de las instalaciones, cumplimiento de normas y procedimientos.



Prueba de los controles

- DESCRIPCIÓN DE PRUEBAS HABITUALES (cont.)

- Seguridad Lógica

- Lectura y comprensión de la política de contraseñas establecida.
- Comprobar el cumplimiento de lo establecido en la política.
- Comprensión de los niveles de identificación de usuarios.
- Revisión de la seguridad lógica del sistema operativo (herramientas automáticas).
- Entrevista con el responsable de la seguridad.



Prueba de los controles

- DESCRIPCIÓN DE PRUEBAS HABITUALES (cont.)
 - Explotación de Sistemas (Operaciones)
 - Entrevistas con los técnicos de sistemas.
 - Verificar el cumplimiento de los controles establecidos (pruebas de cumplimiento).
 - Realizar pruebas sustantivas para aquellos controles no satisfactorios.
 - Mantenimiento
 - Lectura y comprensión de los procedimientos de mantenimiento.
 - Entrevista con los responsables.



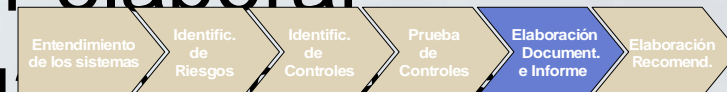
Prueba de los controles

- DESCRIPCIÓN DE PRUEBAS HABITUALES (cont.)
 - Aplicaciones
 - Entrevistas con dirección y usuarios.
 - Realización de encuestas a los usuarios para medir el nivel de satisfacción.
 - Observación del trabajo de los usuarios.
 - Juegos de prueba de datos de entrada.
 - Revisión de las salidas.
 - Recálculos o conciliaciones de datos de entrada y salida.



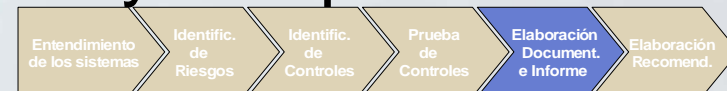
Elaborar la documentación

- La documentación de la auditoría informática es el registro del trabajo de auditoría que se llevó a cabo y de las evidencias que respaldan los hallazgos y las conclusiones.
- El auditor debe entender las técnicas para documentar un sistema de información así como también para documentar la comprensión del entorno de los sistemas.
- El auditor también debe poder elaborar documentos de trabajo adecuados, relevantes,



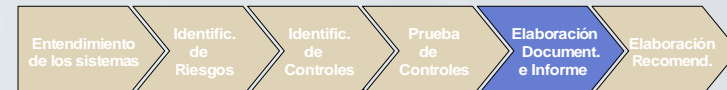
Elaborar la documentación

- Los resultados de un trabajo de auditoría de Sistemas de Información suelen incluir:
 - Mapas de Procesos
 - Descripción de procesos
 - Descripción de pruebas realizadas
 - Resultados obtenidos
 - Informe de auditoría con los hallazgos y las recomendaciones
 - Plan de acción (con la implicación y compromiso del auditado)



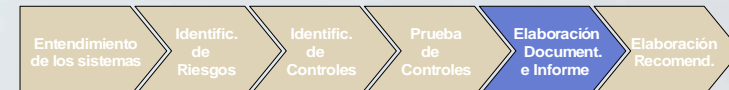
Conclusión de la Auditoría

- Elaboración del informe de auditoría (I)
 - Los puntos esenciales que debe incluir un informe de auditoría son:
 - Identificación del informe
 - Identificación de los destinatarios del informe
 - Identificación de la Entidad auditada
 - Objetivos de la auditoría
 - Deben indicarse claramente aquellos que no se hayan podido cumplir
 - Normativa aplicada y excepciones
 - Alcance de la auditoría
 - Debe incluir el tipo de trabajo realizado con sus limitaciones, el



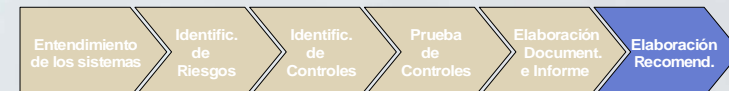
Conclusión de la Auditoría

- Elaboración del informe de auditoría (II)
 - Informe corto de opinión
 - Incluye los resultados del trabajo realizado
 - Informe largo y otros informes
 - Entra en un mayor nivel de detalle en cuanto al trabajo realizado y a los resultados obtenidos
 - Fecha del informe
 - Identificación y firma del auditor
 - Lista de distribución del informe
 - Indicando quién podrá hacer uso de él y con qué fines

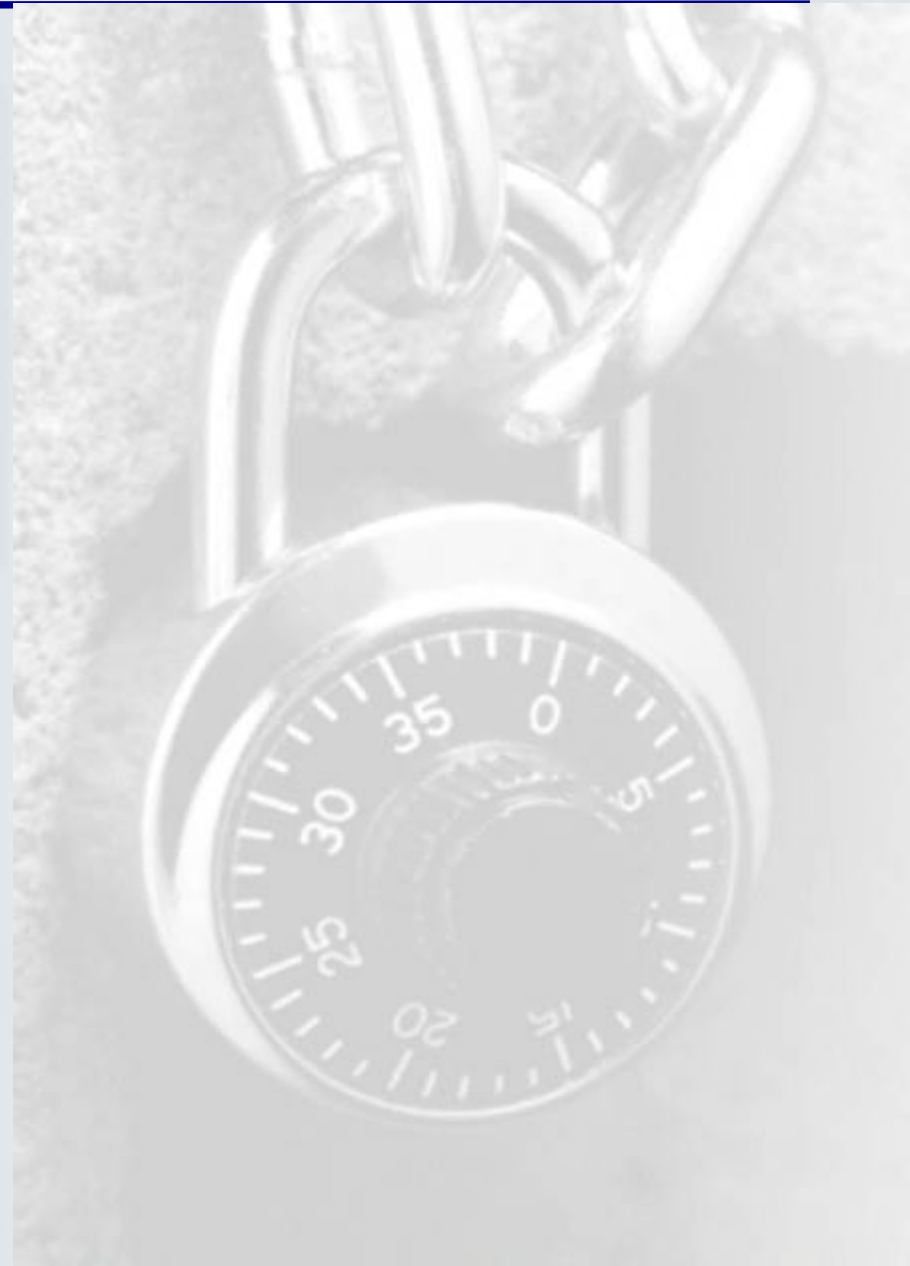


Deloitte. Elaboración de las recomendaciones

- Adicionalmente a las recomendaciones, el auditor puede incluir en su Informe de Auditoría un Plan de Acción que facilite a la gerencia la implementación de las medidas necesarias.
- El Plan de Acción debe ser una relación priorizada de las medidas en función de los acuerdos con los distintos Departamentos / Áreas



Enlaces de interés



- <http://www.isaca.org/>: Information Systems Audit and Control Association (ISACA).
- <http://www.auditoresdesistemas.com/>: Asociación de Auditores y Auditoría y Control de Sistemas y Tecnologías de la Información y las Comunicaciones (ASIA).
- <http://www.csi.map.es/>: Consejo Superior de Informática y para el Impulso de la Administración Electrónica.
- <https://www.agenciaprotecciondatos.org/>: Agencia de Protección de Datos (APD).
- <http://www.acl.com/>: Herramienta para Auditoría de Sistemas de Información
- <http://www.aicpa.org/assurance/trustservices/index.asp>: Trust Services (SysTrust/WebTrust) del American Institute of Certified Public Accountants (AICPA).