TEMA 9 AUDITORIA DE PROYECTO

1. Auditoría:

Procedimiento reglado para analizar cualitativamente y cuantitativamente la eficiencia de un proceso, una tarea o un sistema.

Las auditorias pueden ser internas o externas.

Toda empresa debe tener una auditoria interna.

2. Las funciones de control interno y auditoría informáticos.

2.1 Control Interno Informático.

El Control Interno Informático controla diarimente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la Dirección de la Organización y/o la Dirección de Informática, cumpliendo los requerimientos legales.

La misión del control Interno Informático es asegurarse de que las medidas que se tienen de los mecanismos implantados por cada responsable sean correctas y válidas.

Control Interno Informático suele ser un órgano *staff* de la Dirección del Departamento de Informática y está dotado de las personas y medos materiales proporcionados a los cometidos que se le encomienden.

Como principales objetivos podemos indicar los siguientes:

- Controlas que todas las actividades se realizan cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- Asesorar sobre el conocimiento de las normas.
- Colaborar y apoyar el trabajo de Auditoría Informática, así como de las auditorías externas al Grupo.
- Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio informático, lo cual no debe considerarse como que la implantación de los mecanismos de medida y la responsabilidad del logro de esos niveles se ubique exclusivamente en la función de Control Interno, sino que cada responsable de objetivos y recursos es responsable de esos niveles, así como de la implantación de los medios de medida adecuados.

Realizar en los diferentes sistemas (centrales, departamentales, redes locales, PC´s, etc:) y entornos informáticos (producción, desarrollo o pruebas) el control de las diferentes actividades operativas sobre:

- El cumplimiento de procedimiento, normas y controles dictados. Merece resaltarse la vigilancia sobre el control de cambios y versiones del software.
- Controles sobre la producción diaria.

- Controles sobre la calidad y eficiencia del desarrollo y mantenimiento del software y del servicio informático.
- Controles en las redes de comunicaciones.
- Controles sobre el software de base.
- Controles en los sistemas microinformáticos
- La seguridad informática (su responsabilidad puede estar asignada a control interno o bien pueda asignársele la responsabilidad de control dual de la misma cando está encargada a otro órgano):

    - Usuarios, responsables y perfiles de uso de archivos y bases de datos.
    - Normas de seguridad
    - Control de información clasificada
    - Control dual de la seguridad informática

- Licencias y relaciones contractuales con terceros.
- Asesorar y transmitir cultura sobre el riesgo informático.

2.2 Auditoría Informática.

La Auditoria Informática es el proceso de recoge, 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 eficientes los recursos. De este modo la auditoria informática sustenta y confirma la consecución de los objetivos tradicional de la auditoria:

- Objetivos de protección de activos e integridad de datos.
- Objetivos de gestión que abarcan, no solamente los de protección de activos sino también los de eficacia y eficiencia.

El auditor evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informáticos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso del software. En muchos casos, ya no es posible verificar manualmente los procedimientos informatizados que resumen calculan y clasifican datos, por lo que se deberá emplear software de auditoría y otras técnicas asistidas por ordenador.

El auditor es responsable de revisar e informar a la Dirección de la Organización sobre el diseño y el funcionamiento de los controles implandos y sobre la fiabilidad de la información suministrada.

Se pueden establecer tres grupos de funciones a realizar por un auditor informático.

- Participar en las revisiones durante y después del diseño, realización, implantación y explotación de aplicaciones informáticas, así como en las fases análogas de realización de cambios importantes.

- Revisar y juzgar los controles implantados en los sistemas informativos o para verificar su adecuación a las órdenes e instrucciones de Dirección, requisitos legales, protección de confidencialidad y cobertura ante errores y fraudes.
- Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos e información.

2.3 Control interno y auditoría informáticos: campos análogos.

La evolución de ambas funciones ha sido espectacular durante la última década. Muchos controles internos fueron una vez auditores. De hecho, muchos de los actuales responsables de control interno informático recibieron formación en seguridad informática tras su paso por la formación en auditoría. Numerosos auditores se pasan al campo de control interno informático debido a la similitud de los objetivos profesionales de control y auditoria, campos análogos que propician una transición natural.

Aunque ambas figuras tientes objetivos comunes, existen diferencias que conviene matizar:

Similitudes entre Control Interno Informático y Auditor Informático

- *Personal interno*
- *Conocimientos especializados en Tecnología de la Información*
- *Verificación del cumplimiento de controles internos, normativa y procedimientos establecidos por la Dirección de Informática y la Dirección General para los sistemas de información.*

Diferencias entre Control Interno Informático y Auditor Informático

C.I.I.

- *Análisis de los controles en el día a día.*
- *Informa a la Dirección del Departamento de Informática*
- *Solo personal interno*
- *El alcance de sus funciones es unicamente sobre el Departamento de Informática.*

A.I.

- *Análisis de un momento informático determinado*
- *Informa a la Dirección General de la Organización*
- *Personal interno y/o externo*
- *Tiene cobertura sobre todos los componentes de los sistemas de información de la Organización.*

3. Sistema De Control Interno Informático.

3.1. Definición y tipos de controles internos

Se puede definir el control interno como "cualquier actividad o acción realizada manual y/o automáticamente parra prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos".

Los controles cuando se diseñen, desarrollen e implanten han de ser al menos completos, simples, fiables, revisables, adecuados y rentables. Respecto a esto ultimo habrá que analizar el coste-riesgo de su implantación.

Los controles internos que se utilizan en el entorno informático continúan evolucionando hoy en día a medida que los sistemas informáticos se vuelven complejos. Los progresos que se producen en la tecnología de soportes físicos y de software han modificado de manera significativa los procedimentos que se empleaban tradicionalmente para controlar los procesos de aplicaciones y para gestionar los sistemas de información.

Para asegurar la integridad, disponibilidad y eficacia de los sistemas se requieren complejos mecanismos de control, la mayoría de los cuales son automáticos. Resulta interesante observar, sin embargo, que hasta en los sistemas servidor/cliente avanzados, aunque algunos controles son completamente automáticos, otros son completamente manuales, y muchos dependen de una combinación de elementos de software de procedimientos.

Históricamente, los objetivos de los controles informáticos se han clasificado en las siguientes categorías:

- Controles preventivos: para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.
- Controles detectivos: cuando fallan los preventivos para tratar de conocer cuanto antes el evento. Por ejemplo, el registro de intentos de acceso no autorizados, el registro de la actividad diaria para detectar errores u omisiones, etc.
- Controles correctivos: facilitan la vuelta a la normalidad cuando se han producido incidencias, por ejemplo, la recuperación de un fichero dañado a partir de las copias de seguridad.

Como el concepto de controles se originó en la profesión de auditoría, resulta importante conocer la relación que existe entre los métodos de control, los objetivos de control y los objetivos de auditoría. Se trata de un tema difícil por el hecho de que, históricamente, cada método de control ha estado asociado unívocamente con un objetivo de control (por ejemplo, la seguridad de ficheros de datos se conseguía sencillamente manteniendo la sala de ordenadores cerrada con llave).

Sin embargo, a medida que los sistemas informáticos se han vuelto más complejos, los controles informáticos han evolucionado hasta convertirse en procesos integrados en los que se atenúan las diferencias entre las categorías tradicionales de controles informáticos.

Por ejemplo, en los actuales sistemas informáticos puede resultar difícil ver la diferencia entre seguridad de los programas, de los datos y objetivos de control del software del sistema, porque el mismo grupo de métodos de control satisface casi totalmente los tres objetivos de control.

La relación que existe entre los métodos de control y los objetivos de control puede demostrarse mediante el siguiente ejemplo, en el que un mismo conjunto de métodos de control se utiliza para satisfacer objetivos de control tanto de mantenimiento como de seguridad de los programas:

- Objetivo de control de mantenimiento: asegurar que las modificaciones de los procedimientos programados están adecuadamente diseñadas, probadas, aprobadas e implantadas.
- Objetivo de control de seguridad de programas: garantizar que no se pueden efectuar cambio no autorizados en los procedimientos programados

4. IMPLANTACIÓN DE UN SISTEMA DE CONTROLES INTERNOS INFORMÁTICOS

Los controles pueden implantarse a varios niveles diferentes. Exige analizar diversos elementos interdependientes.
Para llegar a conocer bien la configuración del sistema se hace necesario documentar los detalles relacionados con :

Entorno de red: Esquema de la red
Descripción de la configuración hardware de comunicaciones
Descripción del sw utilizado como acceso a las telecomunicaciones
Control de red
Situación general de los ordenadores

Configuración del ordenador base: Configuración del soporte físico
Entorno del S.O
Software con particiones
Entornos (pruebas y real)
Bibliotecas de programas y conjuntos de datos

Entorno de aplicaciones: Procesos de transacciones
Sistemas de gestión de BD
Entornos de procesos distribuidos

Productos y herramientas: Software para el desarrollo de programas
Sw de gestión de bibliotecas y para operaciones automáticas

Seguridad del ordenador base: Identificar - verificar usuarios = control de acceso
Registro e información
Integridad del sistema
Controles de supervisión

Para la implantación de un sistema de controles internos informáticos habrá que definir:

- La Gestión de los sistemas de información = políticas, reglas, normas, pautas..
- La Administración de sistemas = controles sobre la actividad.
- Seguridad = incluye tres clases de controles: integridad, confidencialidad y disponibilidad.
- Gestión del cambio = separación de las pruebas y la producción sw

La implantación de una política y cultura sobre la seguridad necesita de varias fases y que esté respaldada por la Dirección. Etapas:

- Dirección de Negocio o de Sistema de Información (S.I.) = define la política y directrices del S.I en función de las exigencias del negocio(internas o externas).
- Dirección de Informática = define las normas de funcionamiento del entorno informático y de cada una de las funciones de informática.
- Control Interno Informático = define los controles periódicos que se realizan a cada función informática. Revisión periódica de los controles establecidos de Control Interno Informático informando de las desviaciones a la Dirección y sugiriendo cambios. Transmitirá a toda la organización de Informática la cultura y políticas del riesgo informático.
- Auditor interno/externo informático = revisa los controles internos definidos en cada función informática y el cumplimiento de la normativa interna y externa, de acuerdo con los objetivos definidos por la Dirección de Negocio y de Informática. Informará de los hechos observados y recomendará acciones que minimicen los riesgos que pueden producirse.

A continuación se indican algunos controles internos para sistemas de información =

1. *Controles generales organizativos* : políticas, planificación, estándares, procedimientos, organizar el departamento de informática, descripción de las funciones y responsabilidades, políticas de personal, asegurar que se revisan los informes de control, asegurar existencia de una política de clasificación de información, definir la figura del Control Interno Informático y de Auditoría informática
2. *Controles de desarrollo, adquisición y mantenimiento de información* : permiten alcanzar la eficacia del sistema, economía y eficiencia, integridad de los datos, protección de los recursos y cumplimiento con las leyes y regulaciones.
   -empleo de una metodología del ciclo de vida del desarrollo de sistemas
   -explotación y mantenimiento :control de la explotación, sistema de contabilidad, seguimiento y control de los cambios
3. *Controles de explotación de S.I* : planificación y gestión de recursos, controles para el uso efectivo de recursos, procedimientos de selección, instalación, mantenimiento, seguridad y control de cambios del software, seguridad física y lógica.
4. *Controles en aplicaciones :* cada aplicación lleva controles para garantizar la entrada, actualización, validez, y mantenimiento de los datos.
5. *Controles específicos de ciertas tecnologías* : controles en Sistemas de Gestión de BD, controles en informática distribuida y redes, controles sobre PCs y redes de área local.

AUDITORÍA DE PROYECTOS DE DESARROLLO DE S.I.:

Objetivos y técnicas de control generales aplicables a cualquier proyecto; que aplica el auditor a medida que avanza el proyecto o bien una vez finalizado.

APROBACIÓN, PLANIFICACIÓN Y GESTIÓN DEL PROYECTO:

OBJETIVO DE CONTROL B1: El proyecto de desarrollo debe estar aprobado, definido y planificado formalmente.

C-B1-1: Debe existir una orden de aprobación del proyecto que defina claramente los objetivos, restricciones y las unidades afectadas.

- Orden de aprobación del proyecto por un organismo competente.
- Definidos correctamente objetivos y restricciones.
- Identifica las unidades de la organización a las que afecta.

C-B1-2: Debe designarse un responsable (director) del proyecto.

- Designación se ha hecho correctamente.
- Se ha comunicado al director su nombramiento y toda la información relevante.

C-B1-3: Debe catalogarse el proyecto y decidir el modelo de ciclo de vida.

- Se ha hecho según las normas.
- Se han evaluado los riesgos.
- Se ha elegido el ciclo de vida adecuado.
- Se ha usado la información histórica.
- Si el modelo es el basado en prototipos, deben cumplirse los requisitos necesarios y debe existir un acuerdo sobre el alcance y objetivo del prototipo.

C-B1-4: Debe elegirse el equipo técnico y se debe determinar el plan del proyecto.

- El director y el equipo de desarrollo se han designado correctamente.
- Participantes de otras áreas se han solicitado según protocolo.
- Personal externo con perfil adecuado y contrato según protocolo.
- Se ha comunicado a todo el equipo los objetivos, responsabilidad de cada uno, fechas de participación y dedicación (completa/parcial).
- El plan de proyecto es realista y utiliza información histórica para estimar.

OBJETIVO DE CONTROL B2: El proyecto debe gestionarse de forma que se consigan los mejores resultados teniendo en cuenta las restricciones de tiempo y recursos.

C-B2-1: Los responsables de las unidades o áreas afectadas por el proyecto deben participar en la gestión del mismo.

- Se ha constituido formalmente el comité de dirección del proyecto y en él se han incluido los responsables de las áreas afectadas.
- El comité se reúne períodicamente y tiene competencia para asignar recursos, revisar la marcha y modificar el plan del proyecto.
- Las reuniones se hacen con un orden del día previo y las decisiones en ellas quedan reflejadas en acta.
- El número de reuniones y la duración no superan un límite razonable en función de la envergadura del proyecto.

C-B2-2: Debe establecerse un mecanismo para la resolución de problemas.

- Existen hojas de registro de problemas y un responsable de su recepción, así como un procedimiento de tramitación.
- Hay método para catalogar y dar prioridad a los problemas, así como para trasladarlos al responsable de su resolución y comunicarlos al director y al comité de dirección.
- Se controla la solución del problema y se deja documentada.

C-B2-3: Debe existir un control de cambios.

- Existe un mecanismo para registrar los cambios, así como para evaluar su impacto.
- La documentación se actualiza y se controlan las versiones de cada producto, consignando la fecha última de actualización.
- Se remite la documentación actualizada a todos los participantes del proyecto.

C-B2-4: Si se reajusta el plan del proyecto (final de fase) se hace correctamente.

- Se respetan los límites temporales y presupuestarios marcados al inicio del proyecto, o por el contrario es aprobado por el comité de dirección.
- Se han tenido en cuenta los riesgos del reajuste.
- Se ha usado la información histórica del área sobre estimaciones.
- Se notifica el cambio a todas las personas del proyecto afectadas.
- Si existe un plan de sistemas, se actualizará en consecuencia.

C-B2-5: Debe hacerse un seguimiento de los tiempos empleados por tareas como a lo largo del proyecto.

- Existe un procedimiento que permita registrar los tiempos que cada participante dedica y que tarea realiza.
- Las productividades de los empleados son similares y en consonancia con la información histórica.

C-B2-6: Debe controlarse que se siguen las etapas del ciclo de vida y que se generan todos los documentos asociados.

- Antes de comenzar una etapa se ha documentado, revisado y aceptado la previa.
- La documentación sigue los estándares.
- Se respeta el plan o por el contrario se procede a su modificación.
- Se respeta el uso de recursos establecido.

C-B2-7: Cuando termina el proyecto se debe cerrar toda la documentación, liberar los recursos y hacer balance.

- La documentación es completa y catalogada.
- Los recursos se ponen a disposición del área de la que provienen.
- El comité de dirección y el director hacen balance, toda esta información se registra en los archivos históricos.
- La nueva aplicación se incorpora al catálogo de aplicaciones con toda la información relevante.

AUDITORÍA DE LA FASE DE ANÁLISIS:

Pretende obtener un conjunto de especificaciones formales que describan las necesidades de información que deben ser cubiertas por el nuevo sistema de una forma independiente del entorno técnico.

Análisis de Requisitos del Sistema (ARS):

Se identifican los requisitos del nuevo sistema, distinguiendo su importancia y prioridad. Se determinan las posibles soluciones alternativas y se elige la más adecuada.

OBJETIVO DE CONTROL C1: Los usuarios y responsables establecerán los requisitos.

C-C1-1: Deben participar usuarios de todas las unidades a las que afecta el sistema.

- Existe un documento aprobado por el comité de dirección en el que se determina el grupo de usuarios que participan en el proyecto.
- Los usuarios son suficientemente representativos.
- Se ha comunicado a los usuarios su participación, su responsabilidad y su dedicación estimada.

C-C2-2: Debe realizarse un plan de entrevistas con el grupo de usuarios y con los responsables de las unidades.

- Existe un plan consensuado con el comité de dirección que detalla para cada entrevista la fecha, hora y lugar, tipo de entrevista y un guión.
- Se entrevista a todos los usuarios y a todos los responsables.
- Se remite el guión de la entrevista con tiempo suficiente a los entrevistados para que puedan prepararla o aportar documentación.
- El guión incluye cuestiones para obtener información sobre las funciones del entrevistado y los problemas que necesita resolver.
- Una vez documentadas las entrevistas se contrastan las conclusiones con los entrevistados.

C-C1-3: A partir de las entrevistas se debe documentar el sistema actual así como sus problemas. Debe obtenerse también un catálogo con los nuevos requisitos.

- Se ha realizado un modelo físico del sistema actual, incluyendo objetivos, funciones y flujos de entrada y salida.
- Se han catalogado los problemas del sistema actual.
- Se han realizado el modelo lógico de datos y el de procesos del sistema actual.
- Existe el catálogo de requisitos que están justificados.
- Los requisitos son concretos y cuantificables.
- Cada requisito tiene una prioridad y está clasificado en funcional o no funcional.
- El catálogo de requisitos ha sido revisado y aprobado por el comité de dirección y por los usuarios.

C-C1-4: Debe existir un procedimiento formal para registrar cambios en los requisitos del sistema por parte de los usuarios.

- El procedimiento existe y está aprobado.
- Es coherente con el procedimiento de control de cambio general.

OBJETIVO DE CONTROL C2: Se utiliza la alternativa más favorable para que el sistema cumpla los requisitos.

C-C2-1: Debe definirse las alternativas de construcción con sus ventajas e inconvenientes. Se selecciona la más adecuada.

- Existe un documento en el que se describen las alternativas.
- Hay más de una alternativa, o por el contrario sólo existe 1 real.
- Cada alternativa está descrita desde el punto de vista lógico y es coherente con los requisitos.
- Si existe en el mercado algún producto que cumpla con unas mínimas garantías los requisitos, una de las alternativas debe ser su compra.

- Si no lo impiden las características del proyecto una de las alternativas debe ser el desarrollo del sistema por una empresa externa.
- Se ha evaluado las ventajas e inconvenientes de cada alternativa de forma objetiva así como sus riesgos.
- El comité de dirección ha seleccionado una alternativa y es la mejor.

C-C2-2: La actualización del plan de proyecto seguirá los criterios comentados.

Especificación Funcional del Sistema (EFS):

OBJETIVO DE CONTROL D1: El nuevo sistema debe especificarse completamente desde el punto de vista funcional y aprobado por los usuarios.

C-D1-1: Debe realizarse un Modelo Lógico de Procesos (MLP) y un Modelo Lógico de Datos (MLD).

C-D1-2: Debe existir el diccionario de datos o repositorio.

C-D1-3: Debe definirse la forma en la que el nuevo sistema interactuará con los usuarios.

C-D1-4: La especificación del nuevo sistemas incluye requisitos de seguridad y rendimiento.

C-D1-5: Debe especificarse las pruebas que el nuevo sistema debe superar para ser aceptado.

C-D1-6: La actualización del plan de proyecto seguirá los criterios comentados.

AUDITORÍA DE LA FASE DE DISEÑO:

Se elaborará el conjunto de especificaciones físicas del nuevo sistema.

Diseño Técnico del Sistema (DTS):

Se diseñará la arquitectura del sistema y el esquema externo de datos.

OBJETIVO DE CONTROL E1: debe definirse una arquitectura física para el sistema coherente con la especificación funcional y el entorno tecnológico.

C-E1-1: El entorno tecnológico debe estar definido de forma clara y conforme a los estándares.

C-E1-2: Identificar todas las actividades físicas a realizar y descomponerlas modularmente.

C-E1-3: Debe diseñarse la estructura física de datos adaptándola al entorno tecnológico.

C-E1-4: Debe diseñarse un plan de pruebas que permita la verificación de los distintos componentes del sistema, los subsistemas y el sistema.

C-E1-5: La actualización del plan de proyecto seguirá los criterios comentados.

AUDITORÍA DE LA FASE DE CONSTRUCCIÓN:

Se programarán y probarán los distintos componentes y se pondrán en marcha los procedimientos para que los usuarios puedan trabajar con el sistema.

Desarrollo de los Componentes del Sistema (DCS):

Se desarrollan los distintos componentes, se prueban individualmente como integrados y se desarrollan los procedimientos de operación.

OBJETIVO DE CONTROL F1: Los componentes o módulos deben desarrollarse utilizando técnicas de programación correctas.

C-F1-1: Debe prepararse el entorno de desarrollo y de pruebas, así como los procedimientos de operación.

C-F1-2: Debe programarse, probar y documentar cada una de los componentes.

C-F1-3: Deben realizarse las pruebas de integración para asegurar que las interfaces entre los componentes o módulos funcionan.

Desarrollo de los Procedimientos de Usuario (DPU):

Se definen los procedimientos y formación para que los usuarios puedan utilizar el nuevo sistema. Instalación, conversión de datos y operación/explotación.

OBJETIVO DE CONTROL G1: Los futuros usuarios deben estar capacitados y disponer de los medios para hacer buen uso del sistema.

C-G1-1: Desarrollo de los componentes debe estar planificado.

C-G1-2: Debe especificarse los perfiles de usuario.

C-G1-3: Deben desarrollarse todos los procedimientos de usuario con arreglo a los estándares.

C-G1-4: Deben definirse los procesos de formación o selección de personal.

C-G1-5: Deben definirse los recursos materiales necesarios para el trabajo de los usuarios.

AUDITORÍA DE LA FASE DE IMPLANTACIÓN:

Se realiza la aceptación del sistema por parte de los usuarios y las actividades de puesta en marcha.

Pruebas, Implantación y Aceptación del Sistema (PIA):

Se verifica que el sistema cumple con los requisitos establecidos. Ya probado y aceptado, se pondrá en explotación.

OBJETIVO DE CONTROL H1: El sistema debe ser aceptado formalmente por los usuarios antes de ser puesto en explotación.

C-H1-1: Deben realizarse las pruebas del sistema que se especificaron.

C-H1-2: Debe revisarse el plan de implantación y aceptación para adaptarlo al final del proyecto.

C-H1-3: Debe aceptarse el sistema por los usuarios antes de ponerse en explotación.

OBJETIVO DE CONTROL H2: El sistema se pondrá en explotación formalmente y pasará a estar en mantenimiento sólo cuando haya sido aceptado y esté preparado.

C-H2-1: Deben instalarse todos los procedimientos de explotación.

C-H2-2: El sistema nuevo se pondrá en explotación de forma coordinada con la retirada del antiguo (si existe) migrando los datos si es necesario.

C-H2-3: Debe firmarse el final de la implantación por parte de los usuarios.

C-H2-4: Debe supervisarse el trabajo de los usuarios durante las primeras semanas.

C-H2-5: Para terminar el proyecto se pondrá en marcha el mecanismo de mantenimiento.