CAPÍTULO 12

AUDITORÍA DEL DESARROLLO

José Antonio Rodero Rodero

12.1. INTRODUCCIÓN

La necesidad de que una organización cuente con procedimientos de control interno es aceptada ampliamente como garantía de una gestión eficaz orientada a la consecución de los objetivos marcados. La función auditora es precisamente la encargada de comprobar la existencia de estos procedimientos de control y de verificar su correcta definición y aplicación, determinando las deficiencias que existan al respecto y los riesgos asociados a estas carencias de control.

Teniendo en cuenta que cada organización puede descomponerse funcionalmente en distintos departamentos, áreas, unidades, etc., es necesario que los mecanismos de control interno existan y se respeten en cada una de las divisiones funcionales para que éstas cumplan adecuadamente su cometido y hagan posible que la organización en su conjunto funcione de manera correcta.

Aplicando la división funcional al departamento de informática de cualquier entidad, una de las áreas que tradicionalmente aparece es la de desarrollo. Esta función abarca todas las fases que se deben seguir desde que aparece la necesidad de disponer de un determinado sistema de información hasta que éste es construido e implantado. Para delimitar el ámbito de este capítulo sobre auditoría del desarrollo, se entenderá que el desarrollo incluye todo el ciclo de vida del software excepto la explotación, el mantenimiento y la retirada de servicio de las aplicaciones cuando ésta tenga lugar.

Si se entiende por ingeniería del software "el establecimiento y uso de principios de ingeniería robustos, orientados a obtener software económico que sea fiable, cumpla los requisitos previamente establecidos y funcione de manera eficiente sobre

máquinas reales" (Fritz Bauer), la auditoría del desarrollo tratará de verificar la existencia y aplicación de procedimientos de control adecuados que permitan garantizar que el desarrollo de sistemas de información se ha llevado a cabo según estos principios de ingeniería, o por el contrario, determinar las deficiencias existentes en este sentido.

El planteamiento de este capítulo está orientado al desarrollo de sistemas de información en el sentido tradicional, sin que se hayan tenido en cuenta las peculiaridades del desarrollo de otro tipo de software como puedan ser sistemas operativos, software de comunicaciones, software empotrado, etc. Tampoco se ha tenido en cuenta la gestión de la calidad en el desarrollo, pues hay un capítulo dedicado a tal efecto, ni conceptos generales de control interno y auditoría que ya se abordaron en la parte I del libro (por ejemplo, criterios para la realización del informe, recomendaciones en el trato con los auditados, necesidad de independencia del auditor, preparación y realización de las entrevistas, etc.).

12.2. IMPORTANCIA DE LA AUDITORÍA DEL DESARROLLO

Aunque cualquier departamento o área de una organización es susceptible de ser auditado, hay una serie de circunstancias que hacen especialmente importante al área de desarrollo y, por tanto, también su auditoría, frente a otras funciones o áreas dentro del departamento de informática:

- Los avances en tecnologías de los computadores han hecho que actualmente el desafío más importante y el principal factor de éxito de la informática sea la mejora de la calidad del software.

- El gasto destinado a software es cada vez superior al que se dedica a hardware.

- A pesar de la juventud de la ciencia informática, hace años que se produjo la denominada "crisis del software". Incluye problemas asociados con el desarrollo y mantenimiento del software y afecta a un gran número de organizaciones. En el área del hardware no se ha dado una crisis equivalente.

- El software como producto es muy difícil de validar. Un mayor control en el proceso de desarrollo incrementa la calidad del mismo y disminuye los costes de mantenimiento.

- El índice de fracasos en proyectos de desarrollo es demasiado alto, lo cual denota la inexistencia o mal funcionamiento de los controles en este proceso. Los datos del Government Accounting Office Report (EE.UU.) sobre diversos proyectos de software (valorados en 6,8 millones de dólares) son ilustrativos:

Un 1.5 % se usó tal y como se entregó.
Un 3.0 % se usó después de algunos cambios.
Un 19.5 % se usó y luego se abandonó o se rehizo.
Un 47 % se entregó pero nunca se usó.
Un 29 % se pagó pero nunca se entregó.

- Las aplicaciones informáticas, que son el producto principal obtenido al final del desarrollo, pasan a ser la herramienta de trabajo principal de las áreas informatizadas, convirtiéndose en un factor esencial para la gestión y la toma de decisiones.

12.3. PLANTEAMIENTO Y METODOLOGÍA

Para tratar la auditoría del área de desarrollo es necesario, en primer lugar, acotar las funciones o tareas que son responsabilidad del área. Teniendo en cuenta que puede haber variaciones de una organización a otra, las funciones que tradicionalmente se asignan al área de desarrollo son:

- Planificación del área y participación, en la medida que corresponda, en la elaboración del plan estratégico de informática.

- Desarrollo de nuevos sistemas. Ésta es la función principal y la que da sentido al área de desarrollo. Incluirá para cada uno de los sistemas, el análisis, diseño, construcción e implantación. El mantenimiento se supondrá función de otra área.

- Estudio de nuevos lenguajes, técnicas, metodologías, estándares, herramientas, etc. relacionados con el desarrollo y adopción de los mismos cuando se considere oportuno para mantener un nivel de vigencia adecuado a la tecnología del momento.

- Establecimiento de un plan de formación para el personal adscrito al área.

- Establecimiento de normas y controles para todas las actividades que se realizan en el área y comprobación de su observancia.

Una vez conocidas las tareas que se realizan en el área de desarrollo, se abordará la auditoría de la misma desglosándola en dos grandes apartados, que más tarde se subdividirán con más detalle:

- Auditoría de la organización y gestión del área de desarrollo.
- Auditoría de proyectos de desarrollo de sistemas de información.

De estos dos apartados se hará más énfasis en el segundo por tratarse de la función principal del área, aunque ha de tenerse en cuenta que una buena organización y gestión es imprescindible para que los proyectos tengan una calidad aceptable.

La metodología que se aplicará es la propuesta por la ISACA (Information Systems Audit and Control Association), que está basada en la evaluación de riesgos: partiendo de los riesgos potenciales a los que está sometida una actividad, en este caso el desarrollo de un sistema de información, se determinan una serie de objetivos de control que minimicen esos riesgos.

Para cada objetivo de control se especifican una o más técnicas de control, también denominadas simplemente controles, que contribuyan a lograr el cumplimiento de dicho objetivo. Además, se aportan una serie de pruebas de cumplimiento que permitan la comprobación de la existencia y correcta aplicación de dichos controles. El esquema para cada objetivo de control es:

...
OBJETIVO DE CONTROL X: ...
C-X-l: Técnica de control *l* del objetivo de control *x* ...
- Pruebas de cumplimiento de C-X-1

C-X-m: Técnica de control *m* del objetivo de control *x* ...
- Pruebas de cumplimiento de C-X-m

...

Una vez fijados los objetivos de control, será función del auditor determinar el grado de cumplimiento de cada uno de ellos. Para cada objetivo se estudiarán todos los controles asociados al mismo, usando para ello las pruebas de cumplimiento propuestas. Con cada prueba de cumplimiento se obtendrá alguna evidencia, bien sea directa o indirecta, sobre la corrección de los controles. Si una simple comprobación no ofrece ninguna evidencia, será necesaria la realización de exámenes más profundos.

En los controles en los que sea impracticable una revisión exhaustiva de los elementos de verificación, bien porque los recursos de auditoría sean limitados o porque el número de elementos a inspeccionar sea muy elevado, se examinará una muestra representativa que permita inferir el estado de todo el conjunto.

El estudio global de todas las conclusiones, pruebas y evidencias obtenidas sobre cada control permitirán al auditor obtener el nivel de satisfacción de cada objetivo de control, así como cuáles son los puntos fuertes y débiles del mismo. Con esta información, y teniendo en cuenta las particularidades de la organización en estudio, se determinará cuáles son los riesgos no cubiertos, en qué medida lo son y qué

consecuencias se pueden derivar de esa situación. Estas conclusiones, junto con las recomendaciones formuladas, serán las que se plasmen en el informe de auditoría.

En los apartados siguientes se agrupan los distintos objetivos de control en varias series, detallándose para cada uno de ellos sus controles asociados y pruebas de cumplimiento. El esquema seguido es el siguiente:

- Organización y gestión del área de desarrollo (serie A, aptdo. 4)
- Proyectos de desarrollo de sistemas de información
  Aprobación, planificación y gestión del proyecto (serie B, aptdo. 5.1)
  Análisis
    Análisis de requisitos (serie C, aptdo. 5.2.1)
    Especificación funcional (serie D, aptdo. 5.2.2)
  Diseño
    Diseño técnico (serie E, aptdo. 5.3.1)
  Construcción
    Desarrollo de componentes (serie F, aptdo. 5.4.1)
    Desarrollo de procedimientos de usuario (serie G, aptdo. 5.4.2)
  Implantación
    Pruebas, implantación y aceptación (serie H, aptdo. 5.5.1)

12.4. AUDITORÍA DE LA ORGANIZACIÓN Y GESTIÓN DEL ÁREA DE DESARROLLO

Aunque cada proyecto de desarrollo tenga entidad propia y se gestione con cierta autonomía, para poderse llevar a efecto necesita apoyarse en el personal del área y en los procedimientos establecidos. La importancia de estos aspectos ha motivado que se dedique un apartado exclusivo a la organización y gestión del área de desarrollo. Se consideran ocho objetivos de control (serie A):

OBJETIVO DE CONTROL A1: El área de desarrollo debe tener unos cometidos asignados dentro del departamento y una organización que le permita el cumplimiento de los mismos.

C-A1-1: Deben establecerse de forma clara las funciones del área de desarrollo dentro del departamento de informática. Se debe comprobar que:

- Existe el documento que contiene las funciones que son competencia del área de desarrollo, que está aprobado por la dirección de informática y que se respeta.

C-AI-2: Debe especificarse el organigrama con la relación de puestos del área, así como el personal adscrito y el puesto que ocupa cada persona. Debe existir un procedimiento para la promoción de personal. Se debe comprobar que:

- Existe un organigrama con la estructura de organización del área. Para cada puesto debe describir las funciones a desempeñar, los requisitos mínimos de formación y experiencia, y la dependencia jerárquica del mismo.
- Existe un manual de organización que regula las relaciones entre puestos.
- Existe la relación de personal adscrito al área, incluyendo el puesto ocupado por cada persona. Se deben cumplir los requisitos de los puestos.
- Están establecidos los procedimientos de promoción de personal a puestos superiores, teniendo siempre en cuenta la experiencia y formación.

C-AI-3: El área debe tener y difundir su propio plan a corto, medio y largo plazo, que será coherente con el plan de sistemas, si éste existe. Se debe comprobar que:

- El plan existe, es claro y realista.
- Los recursos actuales, más los que esté planificado que se incorporen al área, son suficientes para su cumplimiento.
- Se revisa y actualiza con periodicidad en función de las nuevas situaciones.
- Se difunde a todos los empleados para que se sientan partícipes del mismo, al resto del departamento y a los departamentos a los que les atañe.

C-AI-4: El área de desarrollo llevará su propio control presupuestario. Se debe comprobar que:

- Se hace un presupuesto por ejercicio, y se cumple.
- El presupuesto está en consonancia con los objetivos a cumplir.

OBJETIVO DE CONTROL A2: El personal del área de desarrollo debe contar con la formación adecuada y estar motivado para la realización de su trabajo.

C-A2-1: Deben existir procedimientos de contratación objetivos. Se debe comprobar que:

- Las ofertas de puestos del área se difunden de forma suficiente fuera de la organización y las selecciones se hacen de forma objetiva.

- Las personas seleccionadas cumplen los requisitos del puesto al que acceden.

C-A2-2: Debe existir un plan de formación que esté en consonancia con los objetivos tecnológicos que se tengan en el área. Se debe comprobar que:

- Se tiene aprobado un plan de formación a corto, medio y largo plazo que sea coherente con la política tecnológica.

- Incluye toda la información relevante para cada actividad formativa: fechas, horarios, lugar, ponentes, asistentes, material, medios necesarios, etc.

- Las actividades formativas se evalúan por parte de los asistentes y esta evaluación se tiene en cuenta a la hora de redefinir el plan de formación.

Contempla la formación de todos los empleados y tiene en cuenta el puesto que ocupan.

El plan de trabajo del área tiene en cuenta los tiempos de formación.

C-A2-3: Debe existir un protocolo de recepción/abandono para las personas que se incorporan o dejan el área. Se debe comprobar que:

- El protocolo existe y se respeta para cada incorporación/abandono.

- Para la incorporación, incluye al menos los estándares definidos, manual de organización del área, definición de puestos, etc.

- En los abandonos de personal se garantiza la protección del área.

C-A2-4: Debe existir una biblioteca y una hemeroteca accesibles por el personal del área. Se debe comprobar que:

- Están disponibles un número suficiente de libros, publicaciones periódicas, monogramas, etc. de reconocido prestigio y el personal tiene acceso a ellos.

C-A2-5: El personal debe estar motivado en la realización de su trabajo. Este aspecto es difícil de valorar y no es puramente técnico. Se debe comprobar que:

- Existe algún mecanismo que permita a los empleados hacer sugerencias sobre mejoras en la organización del área.

- No existe una gran rotación de personal y hay un buen ambiente de trabajo.

- El rendimiento del personal no cae por debajo de unos mínimos razonables y el absentismo laboral es similar al del resto de la organización.

OBJETIVO DE CONTROL A3: Si existe un plan de sistemas, los proyectos que se lleven a cabo se basarán en dicho plan y lo mantendrán actualizado.

C-A3-1: La realización de nuevos proyectos debe basarse en el plan de sistemas en cuanto a objetivos, marco general y horizonte temporal. Se debe comprobar que:

- Las fechas de realización coinciden con las del plan de sistemas.

- La documentación relativa a cada proyecto que hay en el plan de sistemas se pone a disposición del director de proyecto una vez comenzado el mismo. Esta información debe contener los objetivos, los requisitos generales y un plan inicial.

C-A3-2: El plan de sistemas debe actualizarse con la información que se genera a lo largo de un proceso de desarrollo. Se debe comprobar que:

- Los cambios en los planes de los proyectos se comunican al responsable de mantenimiento del plan de sistemas por las implicaciones que pudiera tener.

OBJETIVO DE CONTROL A4: La propuesta y aprobación de nuevos proyectos debe realizarse de forma reglada.

C-A4-1: Debe existir un procedimiento para la propuesta de realización de nuevos proyectos. Se debe comprobar que:

- Existe un mecanismo para registrar necesidades de desarrollo de nuevos sistemas y en todo caso se aportan los siguientes datos: descripción, necesidad, departamento patrocinador, riesgos, marco temporal, coste de la no realización, ventajas que aporta, adaptación a los planes de negocio, etc.

- Se respeta este mecanismo en todas las propuestas.

C-A4-2: Debe existir un procedimiento de aprobación de nuevos proyectos que dependerá de que exista o no plan de sistemas. Si hay un plan de sistemas se debe comprobar que:

- Se parte de las pautas, prioridades y planificación que éste marque para el desarrollo de cada nuevo sistema.

Si no existe plan de sistemas se debe comprobar que:

- Hay un procedimiento para estudiar la justificación y llevar a cabo el estudio de viabilidad de cada nuevo proyecto, incluyendo un análisis coste/beneficio y teniendo siempre como alternativa la no realización del mismo.

- Están designadas a áreas de la organización que tienen competencia para aprobar formalmente la realización y prioridad de los nuevos proyectos, así como el cauce para reasignar prioridades si fuese necesario. La decisión, afirmativa o negativa, se obtendrá en un tiempo razonable y se comunicará a los promotores.

OBJETIVO DE CONTROL A5: La asignación de recursos a los proyectos debe hacerse de forma reglada.

C-A5-1: Debe existir un procedimiento para asignar director y equipo de desarrollo a cada nuevo proyecto. Se debe comprobar que:

- El procedimiento existe y se respeta.

- Se tiene en cuenta a todas las personas disponibles cuyo perfil sea adecuado a los riesgos de cada proyecto y que tengan disponibilidad para participar.

- Existe un protocolo para solicitar al resto de las áreas (sistemas, comunicaciones, etc.) la participación de personal en el proyecto, y se aplica dicho protocolo.

C-A5-2: Debe existir un procedimiento para conseguir los recursos materiales necesarios para cada proyecto. Se debe comprobar que:

- El procedimiento existe y se respeta.

OBJETIVO DE CONTROL A6: El desarrollo de sistemas de información debe hacerse aplicando principios de ingeniería del software ampliamente aceptados.

C-A6-1: Debe tenerse implantada una metodología de desarrollo de sistemas de información soportada por herramientas de ayuda (CASE). Se debe comprobar que:

La metodología cubre todas las fases del desarrollo y es adaptable a distintos tipos de proyecto.

- La metodología y las técnicas asociadas a la misma están adaptadas al entorno tecnológico y de organización del área de desarrollo.

- Se ha adquirido, homologado e implantado según las normas del área una herramienta CASE que se adapta a la metodología elegida y que cumple con los requisitos mínimos exigibles a una herramienta de este tipo.

- Se ha formado al personal sobre esta metodología y su adaptación, así como sobre las técnicas asociadas y la herramienta CASE.

- Existe un procedimiento que permita determinar en qué proyectos el uso de la herramienta CASE es ventajoso.

- Está claramente especificado de qué forma el uso de la herramienta altera las fases de desarrollo tradicionales.

- La herramienta CASE es capaz de mantener el diccionario de datos.

- La herramienta CASE mantiene los requisitos de confidencialidad necesarios sobre la documentación asociada al proyecto.

C-A6-2: Debe existir un mecanismo de creación y actualización de estándares, así como estándares ya definidos para las actividades principales. Se prestará especial atención a las herramientas y lenguajes de programación no clásicas. Se debe comprobar que:

- El mecanismo para creación de nuevos estándares está documentado y es conocido en el área.

- Hay un estándar para la realización del análisis y diseño, e incluye las técnicas y herramientas a usar, etc.

- Hay un estándar de programación para cada uno de los lenguajes homologados. Se prestará especial atención a las herramientas denominadas RAD (Rapid Application Development), ya que las secuencias posibles de ejecución son muy numerosas (normalmente se activan rutinas por eventos o *triggers* (disparadores) y el orden no se puede prever a priori) y la validación y depuración es prácticamente imposible si no se estandariza la programación.

- Existen convenios sobre los aspectos más importantes de la programación: modularidad, nomenclatura (de funciones, variables, tablas, columnas, etc.), formato de los comentarios, documentación asociada, estilo de programación, etc.

- Hay un estándar general para toda la documentación generada, incluyendo documentación técnica (análisis, diseño, documentación de los programas, cuadernos de carga, etc.), manuales de usuario, procedimientos de operación, etc.

- Hay un estándar para la interfaz de usuario, incluyendo diseño de pantallas, informes, etc.

- Los estándares son conocidos por las personas que deben usarlos y se respetan. Cuando se produce una modificación, ésta se difunde dentro del área.

C-A6-3: Los lenguajes, compiladores, herramientas CASE, software de control de versiones, etc. usados en el área deben ser previamente homologados. Se debe comprobar que:

- Existe un mecanismo para la adquisición y homologación de cualquier nuevo producto software usado en el desarrollo. Se deben evaluar al menos los siguientes parámetros: productividad, portabilidad a otros entornos, transición desde los productos actuales, solvencia del proveedor, riesgo del cambio, cumplimiento de los estándares del área, compatibilidad con el entorno tecnológico (SO, protocolos de comunicaciones, SGBD, etc.), coste, etc.

- Cuando se homologa un nuevo producto de desarrollo se forma al personal del área que lo vaya a manejar.

- Se registra la información más importante acerca de la configuración de los productos recién adquiridos.

- Los productos homologados son suficientes para conseguir los objetivos marcados.

- Periódicamente se comprueba el nivel tecnológico, para ver si es coherente con el plan de sistemas y si está en línea con el de otras organizaciones similares.

C-A6-4: Debe practicarse la reutilización del software. Se debe comprobar que:

- Existe un catálogo con todos los productos software susceptibles de ser reutilizados: librerías de funciones, clases si se utiliza programación orientada a objetos, programas tipo, componentes software, etc.

- El catálogo es conocido y accesible por todos los miembros del área, está actualizado y tiene uno o varios índices que faciliten la búsqueda.

- Existe un catálogo de las aplicaciones disponibles en el área, tanto de las realizadas como de las adquiridas, con toda la información relevante de las mismas.

C-A6-5: Debe existir un método que permita catalogar y estimar los tiempos de cada una de las fases de los proyectos. Se debe comprobar que:

- El método usado es correcto, está bien ajustado y documentado adecuadamente.

- Las desviaciones producidas en cada proyecto se usan para ajustar los parámetros de catalogación y estimación manteniendo un histórico de los mismos.

C-A6-6: Debe existir un registro de problemas que se producen en los proyectos del área, incluyendo los fracasos de proyectos completos. Se debe comprobar que:

- Existe un catálogo de problemas, incluyendo para cada uno de ellos la solución o soluciones encontradas, proyecto en el que sucedió, persona que lo resolvió, etc.

- El catálogo es accesible para todos los miembros del área, está actualizado y tiene uno o varios índices que faciliten la búsqueda.

- Se registran y controlan todos los proyectos fracasados (aquellos que comienzan y no llegan a su fin), así como los recursos invertidos en los mismos.

OBJETIVO DE CONTROL A7: Las relaciones con el exterior del departamento tienen que producirse de acuerdo a un procedimiento.

C-A7-1: Deben mantenerse contactos con proveedores para recibir información suficiente sobre productos que puedan ser de interés. Se debe comprobar que:

- Se está en contacto con un número suficiente de proveedores para recibir una información objetiva y completa, y el tiempo invertido en estas tareas no excede lo razonable.

C-A7-2: Debe existir un protocolo para contratación de servicios externos. Se debe comprobar que:

- Existe el protocolo, está aprobado y se hace uso de él.

- La selección del proveedor se hace de forma objetiva y evita situaciones de monopolio por parte de un único proveedor.

- El protocolo incluye un contrato-tipo que prevea los riesgos más frecuentes cuando se contratan servicios externos, y en todo caso incorpora penalizaciones en caso de incumplimiento de contrato por parte del proveedor.

- El personal externo que intervendrá en los proyectos cumplirá, al menos, los mismos requisitos que se exigen a los empleados del área.

- Una persona del área supervisa el trabajo realizado, certificándolo antes del pago.

- Debe ser compatible con los estándares establecidos en el área.

OBJETIVO DE CONTROL A8: La organización del área debe estar siempre adaptada a las necesidades de cada momento.

C-A8-1: La organización debe revisarse de forma regular. Se debe comprobar que:

- Existe el procedimiento de revisión, se aplica con una periodicidad adecuada y se adapta al dinamismo de la tecnología informática.

- Cuando se reducen modificaciones se documentan, incluyendo la fecha de actualización, y se difunden dentro del área.

12.5. AUDITORÍA DE PROYECTOS DE DESARROLLO DE S.I

Como se planteó en apartados anteriores, cada desarrollo de un nuevo sistema de información será un proyecto con entidad propia. El proyecto tendrá unos objetivos marcados y afectará a determinadas unidades de la organización. Debe tener un responsable y ser gestionado con técnicas que permitan conseguir los objetivos marcados, teniendo en cuenta los recursos disponibles y las restricciones temporales del mismo. En esa gestión deben participar todas las partes de la organización a las que afecte el sistema.

La auditoría de cada proyecto de desarrollo tendrá un plan distinto dependiendo de los riesgos, la complejidad del mismo y los recursos disponibles para realizar la auditoría. Esto obliga a que sean la pericia y experiencia del auditor las que determinen las actividades del proyecto que se controlarán con mayor intensidad en función de los parámetros anteriores.

En este apartado se definirán objetivos y técnicas de control generales aplicables a cualquier proyecto. El auditor decidirá los objetivos más importantes en función de las características del proyecto y de la fase a auditar.

Como se puede observar en el esquema de agrupación de objetivos de control propuesto en el apartado 3, dentro del desarrollo de sistemas de información se han propuesto cinco subdivisiones, entre las cuales se encuentran: análisis, diseño, construcción e implantación. Estas fases, ampliamente aceptadas en ingeniería del software para el desarrollo, son en concreto las que propone la metodología de desarrollo de sistemas de información Métrica versión 2.1.

Además de estas fases, se ha añadido una subdivisión que contiene los objetivos y técnicas de control concernientes a la aprobación, planificación y gestión del proyecto. La aprobación del proyecto es un hecho previo al comienzo del mismo, mientras que la gestión se aplica a lo largo de su desarrollo. La planificación se realiza antes de iniciarse, pero sufrirá cambios a medida que el proyecto avanza en el tiempo.

Aunque los objetivos de control se han catalogado en función de la fase del proyecto a la que se aplican, la auditoría de un proyecto de desarrollo se puede hacer en dos momentos distintos: a medida que avanza el proyecto, o una vez concluido el mismo. Las técnicas a utilizar y los elementos a inspeccionar, normalmente los productos y documentos generados en cada fase del desarrollo, serán los mismos en ambos casos. La única diferencia es que en el primer caso las conclusiones que vaya aportando el auditor pueden afectar al desarrollo del proyecto, aunque nunca participará en la toma de decisiones del mismo.

12.5.1. Aprobación, planificación y gestión del proyecto

Se consideran en este apartado dos objetivos de control (serie B):

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. Se debe comprobar que:

- Existe una orden de aprobación del proyecto refrendada por un órgano competente. El estudio de viabilidad debe haber seguido el cauce establecido.
- En el documento de aprobación están definidos de forma clara y precisa los objetivos del mismo y las restricciones de todo tipo que deben tenerse en cuenta (temporales, recursos técnicos, recursos humanos, presupuesto, etc.).

- Se han identificado las unidades de la organización a las que afecta.

C-BI-2: Debe designarse un responsable o director del proyecto. Se debe comprobar que:

- La designación se ha llevado a cabo según el procedimiento establecido.
- Se le ha comunicado al director su nombramiento junto con toda la información relevante del proyecto.

C-BI-3: El proyecto debe ser catalogado y, en función de sus características, se debe determinar el modelo de ciclo de vida que seguirá. Se debe comprobar que:

- Se ha catalogado y dimensionado el proyecto según las normas establecidas.
- Se han evaluado los riesgos asociados al proyecto, especialmente cuando se van a usar tecnologías no usadas hasta el momento.
- Se ha elegido el ciclo de vida más adecuado al tipo de proyecto de que se trata.
- Se ha hecho uso de la información histórica que se dispone tanto para dimensionar el proyecto y sus riesgos como para seleccionar el ciclo de vida.
- Se prestará especial atención si se elige un ciclo de vida basado en prototipado. En este caso deben cumplirse los requisitos necesarios para aplicarlo con éxito (dificultad de los usuarios para expresar los requisitos y disponibilidad de una herramienta de construcción rápida de prototipos) y debe existir un acuerdo con los usuarios sobre el alcance del prototipo y el objetivo que se persigue con el mismo.

P-BI-4: Una vez determinado el ciclo de vida a seguir, se debe elegir el equipo técnico que realizará el proyecto y se determinará el plan del proyecto. Se debe comprobar que:

- La designación del director del proyecto y del equipo de desarrollo se ha llevado a cabo según el procedimiento establecido.
- Los participantes que pertenezcan a otras áreas (sistemas, comunicaciones, ofimática, etc.) se han solicitado según el protocolo existente.
- Si participa personal externo, los perfiles profesionales son adecuados a las funciones que van a realizar. El contrato cumple el protocolo de contratación.

- Se ha comunicado a todos los miembros del equipo de desarrollo los objetivos del proyecto, la responsabilidad que tendrán en el mismo, las fechas en las que participarán y la dedicación (completa/parcial).

- El plan de proyecto realizado es realista y utiliza la información histórica de la que se disponga para realizar estimaciones.

OBJETIVO DE CONTROL B2: El proyecto se debe gestionar de forma que se consigan los mejores resultados posibles teniendo en cuenta las restricciones de tiempo y recursos. Los criterios usados serán coherentes con los objetivos de las unidades afectadas.

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

- Se ha constituido formalmente el comité de dirección del proyecto y en él están incluidos los responsables de todas las unidades afectadas.

- El comité tiene una periodicidad de reunión mínima, y en cualquier caso siempre que lo exija el desarrollo del proyecto, debe tener competencia para la asignación de recursos, la revisión de la marcha del proyecto y para modificar el plan del proyecto en función de las revisiones.

- Las reuniones se hacen con un orden del día previo y las decisiones tomadas quedan documentadas en las actas de dicho comité.

- El número de reuniones y la duración de las mismas no superan un límite razonable comparado con la envergadura del proyecto.

C-B2-2: Se debe establecer un mecanismo para la resolución de los problemas que puedan plantearse a lo largo del proyecto. Se debe comprobar que:

- Existen hojas de registro de problemas y que hay alguna persona del proyecto encargada de su recepción, así como un procedimiento conocido de tramitación.

- Hay un método para catalogar y dar prioridad a los problemas, así como para trasladarlos a la persona que los debe resolver, informando si es necesario al director del proyecto y al comité de dirección.

- Se controla la solución del problema y se deja constancia de la misma.

C-B2-3: Debe existir un control de cambios a lo largo del proyecto. Se debe comprobar que:

- Existe un mecanismo para registrar los cambios que pudieran producirse, así como para evaluar el impacto de los mismos.
- La documentación afectada se actualiza de forma adecuada y se lleva un control de versiones de cada producto, consignando la última fecha de actualización.
- Se remite la nueva versión de los documentos actualizados a los participantes en el proyecto.

C-B2-4: Cuando sea necesario reajustar el plan del proyecto, normalmente al finalizar un módulo o fase, debe hacerse de forma adecuada. Se debe comprobar que:

- Se respetan los límites temporales y presupuestarios marcados al inicio del proyecto. Si no es así debe ser aprobado por el comité de dirección.
- Se han tenido en cuenta los riesgos del reajuste.
- Se ha hecho uso de la información histórica que se dispone en el área sobre estimaciones.
- Se notifica el cambio a todas las personas que de una u otra forma participen en el proyecto y se vean afectados.
- Si existe un plan de sistemas, se actualizará en consecuencia.

C-B2-5: Debe hacerse un seguimiento de los tiempos empleados tanto por tarea como a lo largo del proyecto. Se debe comprobar que:

- Existe un procedimiento que permita registrar los tiempos que cada participante del proyecto dedica al mismo y qué tarea realiza en ese tiempo.
- Las productividades que se obtienen para distintos empleados en las mismas tareas son similares y están en consonancia con la información histórica.

C-B2-6: Se debe controlar que se siguen las etapas del ciclo de vida adoptado para el proyecto y que se generan todos los documentos asociados a la metodología usada. Se debe comprobar que:

- Antes de comenzar una nueva etapa se ha documentado la etapa previa y se ha revisado y aceptado, especialmente en las fases de análisis y diseño.

- La documentación cumple los estándares establecidos en el área.

- Se respeta el plan establecido y en caso contrario se toman las medidas oportunas o se procede a la aprobación de una modificación del plan.

- Se respeta el uso de recursos previamente establecido.

C-B2-7: Cuando termina el proyecto se debe cerrar toda la documentación del mismo, liberar los recursos empleados y hacer balance. Se debe comprobar que:

- La documentación del proyecto es completa y está catalogada perfectamente para accesos posteriores.

- Los recursos, tanto personales como materiales, se ponen a disposición del área o departamento del que provienen.

- El comité de dirección y el director del proyecto hacen balance del proyecto, estudiando los posibles problemas y sus causas, los cambios de plan, etc. Toda esta información se registra en los archivos históricos sobre estimaciones y problemas.

- La nueva aplicación se incorpora al catálogo de aplicaciones existentes con toda la información relevante de la misma.

12.5.2. Auditoría de la fase de análisis

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.

Esta fase se divide en dos módulos:

12.5.2.1. Análisis de Requisitos del Sistema (ARS)

En este módulo se identificarán los requisitos del nuevo sistema. Se incluirán tanto los requisitos funcionales como los no funcionales, distinguiendo para cada uno de ellos su importancia y prioridad.

A partir del conocimiento del sistema actual y sus problemas asociados, junto con los requisitos que se exigirán al nuevo sistema, se determinarán las posibles soluciones, alternativas que satisfagan esos requisitos y de entre ellas se elegirá la más adecuada. Se consideran dos objetivos de control (serie C):

***OBJETIVO DE CONTROL C1*:** Los usuarios y responsables de las unidades a las que afecta el nuevo sistema establecerán de forma clara los requisitos del mismo.

C-C1-1: En el proyecto deben participar usuarios de todas las unidades a las que afecte el nuevo sistema. Esta participación, que se hará normalmente a través de entrevistas, tendrá especial importancia en la definición de requisitos del sistema. Se debe comprobar que:

- Existe un documento aprobado por el comité de dirección en el que se determina formalmente el grupo de usuarios que participará en el proyecto.
- Los usuarios elegidos son suficientemente representativos de las distintas funciones que se llevan a cabo en las unidades afectadas por el nuevo sistema.
- Se les ha comunicado a los usuarios su participación en el proyecto, informándoles del ámbito del mismo y de qué es lo que se espera de ellos, así como la dedicación estimada que les supondrá esta tarea.

C-C1-2: Se debe realizar un plan detallado de entrevistas con el grupo de usuarios del proyecto y con los responsables de las unidades afectadas que permita conocer cómo valoran el sistema actual y lo que esperan del nuevo sistema. Se debe comprobar que:

- Existe un plan consensuado con el comité de dirección que detalla para cada entrevista la fecha, hora y lugar, tipo de entrevista (individual, en grupo, por escrito, etc.) y un guión de los aspectos que en ella se tratarán.
- Se entrevista a todos los integrantes en el grupo de usuarios y a todos los responsables de las unidades afectadas.
- Se remite el guión a los entrevistados con tiempo suficiente para que éstos puedan preparar la entrevista y la documentación que deseen aportar a la misma.
- El guión incluye todas las cuestiones necesarias para obtener información sobre las funciones que el entrevistado realiza en su unidad y los problemas que necesita resolver.

Una vez documentadas las entrevistas, se contrastan las conclusiones de las mismas con los entrevistados.

C-C1-3: A partir de la información obtenida en las entrevistas, se debe documentar el sistema actual así como los problemas asociados al mismo. Se debe obtener también un catálogo con los requisitos del nuevo sistema. Se debe comprobar que:

- Se ha realizado un modelo físico del sistema actual, incluyendo los objetivos y funciones de cada unidad, así como sus flujos de entrada y salida de información.
- Se han catalogado los problemas del sistema actual así como que estos problemas son reales.
- Se han realizado el modelo lógico de datos y el modelo lógico de procesos del sistema actual, así como que éstos son correctos y que se han llevado a cabo con las técnicas usadas en el área.
- Existe el catálogo de requisitos que están justificados.
- Los requisitos son concretos y cuantificables, de forma que pueda determinarse el grado de cumplimiento al final del proyecto.
- Cada requisito tiene una prioridad y está clasificado en funcional o no funcional.
- El catálogo de requisitos ha sido revisado y aprobado por el grupo de usuarios y por el comité de dirección, constituyendo a partir de este momento el "contrato" entre éstos y el equipo que desarrolla el proyecto.

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

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

OBJETIVO DE CONTROL C2: En el proyecto de desarrollo se utilizará la alternativa más favorable para conseguir que el sistema cumpla los requisitos establecidos.

C-C2-1: Dados los requisitos del nuevo sistema se deben definir las diferentes alternativas de construcción con sus ventajas e inconvenientes. Se evaluarán las alternativas y se seleccionará la más adecuada. Se debe comprobar que:

- Existe un documento en el que se describen las distintas alternativas.
- Hay más de una alternativa, y en caso contrario, que no existe realmente otra posible.
- Cada alternativa está descrita desde un punto de vista lógico (al menos modelo lógico de procesos) y es coherente con los requisitos establecidos.
- Si existe en el mercado al un producto que cumpla con unas mínimas garantías los requisitos especificados, 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 parte de una empresa externa.
- Se han evaluado las ventajas e inconvenientes de cada alternativa de forma objetiva (análisis coste/beneficio por ejemplo), así como los riesgos asociados.
- El comité de dirección ha seleccionado una alternativa como la más ventajosa y es realmente la mejor para la organización.

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

12.5.2.2. Especificación Funcional del Sistema (EFS)

Una vez conocido el sistema actual, los requisitos del nuevo sistema y la alternativa de desarrollo más favorable, se elaborará una especificación funcional detallada del sistema que sea coherente con lo que se espera de él.

La participación de usuarios en este módulo y la realización de entrevistas siguen las pautas ya especificadas en el análisis de requisitos del sistema, por lo que se pasa por alto la comprobación de estos aspectos. El grupo de usuarios y los responsables de las unidades afectadas deben ser la principal fuente de información. Se considera un único objetivo de control (serie D):

OBJETIVO DE CONTROL D1: El nuevo sistema debe especificarse de forma completa desde el punto de vista funcional, contando esta especificación con la aprobación de los usuarios.

C-D1-1: Se debe realizar un modelo lógico del nuevo sistema, incluyendo Modelo Lógico de Procesos (MLP) y Modelo Lógico de Datos (MLD). Ambos deben ser consolidados para garantizar su coherencia. Se debe comprobar que:

- Se ha partido de los modelos realizados en el análisis de requisitos del sistema.
- Existe el MLP, se ha realizado con la técnica adecuada (normalmente diagramas de flujos de datos) y es correcto técnicamente. Describirá qué debe realizar el sistema sin entrar en la forma en que lo hará. Los procesos manuales deben estar diferenciados. Los usuarios deben entender las convenciones de símbolos usadas.
- En el diagrama de contexto están reflejados todos los agentes externos, incluidos otros sistemas con los que el sistema intercambia información. Para cada flujo de datos de entrada o de salida debe estar documentado el contenido, la frecuencia, suceso que lo origina, etc.
- Existe el MLD, se ha realizado con la técnica adecuada (normalmente modelo entidad-relación o diagramas de estructura de datos) y es correcto técnicamente. Debe estar normalizado al menos hasta la tercera forma normal.
- En el MLD están reflejadas todas las entidades con sus atributos y claves, así como las relaciones entre las mismas.
- El MLP y el MLD son coherentes entre sí. La consolidación se debe hacer usando técnicas adecuadas (Historia de la vida de las entidades, por ejemplo).
- El MLP y el MLD han sido aprobados por los usuarios y por el comité de dirección.

C-D1-2: Debe existir el diccionario de datos o repositorio. Se debe comprobar que:

- Existe el diccionario de datos, es correcto y se gestiona de forma automatizada.
- Se respetan en su gestión todos los procedimientos de control de cambios.

C-D1-3: Debe definirse la forma en que el nuevo sistema interactuará con los distintos usuarios. Ésta es la parte más importante para el usuario porque definirá su forma de trabajo con el sistema. Se debe comprobar que:

- Se han descrito con suficiente detalle las pantallas a través de las cuales el usuario navegará por la aplicación, incluyendo todos los campos significativos, teclas de función disponibles, menús, botones, etc. Si hay normas de diseño o estilo de pantallas en el área, se verificará que se respetan.

- Se han descrito con suficiente detalle los informes que se obtendrán del sistema y los formularios asociados, si éstos existen. Si hay normas de diseño o estilo de informes y formularios en el área, se verificará que se respetan.

- La interfaz de usuario se ha aprobado por el grupo de usuarios y por el comité de dirección.

C-D1-4: La especificación del nuevo sistema incluirá los requisitos de seguridad, rendimiento, copias de seguridad y recuperación, etc. Se debe comprobar que:

- Esta información se ha solicitado a los usuarios en las entrevistas correspondientes a este módulo y se ha documentado y contrastado.

- Se han añadido estos requisitos al catálogo de requisitos ya realizado en el ARS.

C-D1-5: Se deben especificar las pruebas que el nuevo sistema debe superar para ser aceptado. Se debe comprobar que:

- Se ha elaborado el plan de pruebas de aceptación del sistema, que éste es coherente con el catálogo de requisitos y con la especificación funcional del sistema y que es aceptado por el grupo de usuarios y por el comité de dirección.

- El plan de pruebas de aceptación tiene en cuenta todos los recursos necesarios.

C-D1-6: La actualización del plan de proyecto seguirá los criterios ya comentados, detallándose en este punto en mayor medida la entrega y transición al nuevo sistema.

12.5.3. Auditoría de la fase de diseño

En la fase de diseño se elaborará el conjunto de especificaciones físicas del nuevo sistema que servirán de base para la construcción del mismo. Hay un único módulo:

12.5.3.1. Diseño Técnico del Sistema (DTS)

A partir de las especificaciones funcionales, y teniendo en cuenta el entorno tecnológico, se diseñará la arquitectura del sistema y el esquema externo de datos. Se considera un único objetivo de control (serie E):

***OBJETIVO DE CONTROL E1*:** Se debe definir una arquitectura física para el sistema coherente con la especificación funcional que se tenga y con el entorno tecnológico elegido.

C-E1-1: El entorno tecnológico debe estar definido de forma clara y ser conforme a los estándares del departamento de informática. Se debe comprobar que:

- Están perfectamente definidos todos los elementos que configuran el entorno tecnológico para el proyecto (servidores, computadores personales, periféricos, sistemas operativos, conexiones de red, protocolos de comunicación, sistemas gestores de bases de datos, compiladores, herramientas CASE, *middleware* en caso de programación cliente/servidor, librerías, etc.).

- Se dispone de los elementos seleccionados, están dentro de los estándares del departamento de informática y son capaces de responder a los requisitos establecidos de volúmenes, tiempos de respuesta, seguridad, etc.

C-E1-2: Se deben identificar todas las actividades físicas a realizar por el sistema y descomponer las mismas de forma modular. Se debe comprobar que:

- Se han documentado todas las actividades físicas que debe realizar el sistema.

- El catálogo de actividades es coherente con las funciones identificadas en el MLP del módulo EFS.

- Se han identificado las actividades que son comunes, así como las que ya existan en las librerías generales del área.

- Existe el documento con el diseño de la estructura modular del sistema, se ha realizado con una técnica adecuada (Diagramas de estructura de cuadros por ejemplo) y es correcto.

- El tamaño de los módulos es adecuado, el factor de acoplamiento entre ellos es mínimo y la cohesión interna de cada módulo es máxima.

- Los módulos se diseñan para poder ser usados por otras aplicaciones si fuera necesario.

- Los componentes o programas del nuevo sistema se han definido con detalle a partir del diseño modular, la definición es correcta y sigue los estándares del área. La descripción de los componentes es suficiente para permitir su programación por parte de un programador sin conocimiento previo del sistema. Se deben especificar los requisitos de operación de los componentes.

- Se han detallado las interfaces de datos y control con otros módulos y sistemas, así como la interfaz de usuario ya especificada en el módulo EFS.

C-EI-3: Se debe diseñar la estructura física de datos adaptando las especificaciones del sistema al entorno tecnológico. Se debe comprobar que:

El modelo físico de datos está basado en el MLD obtenido en el módulo EFS e incluye todas las entidades, relaciones, claves, vistas, etc.

Tiene en cuenta el entorno tecnológico y los requisitos de rendimiento para los volúmenes y frecuencias de acceso estimados.

Si incluye algún incumplimiento de las normas, está justificada.

C-EI-4: Se debe diseñar un plan de pruebas que permita la verificación de los distintos componentes del sistema por separado, así como el funcionamiento de los distintos subsistemas y del sistema en conjunto. Se debe comprobar que:

- Existe el plan de pruebas y contempla todos los recursos necesarios para llevarlas a efecto.

- Las personas que realizarán las pruebas de verificación son distintas a las que han desarrollado el sistema.

- Es adecuado para validar cada uno de los componentes del sistema, incluyendo pruebas del tipo caja blanca para cada módulo. Tendrán en cuenta todas las posibles condiciones lógicas de ejecución, además de posibles fallos del hardware o software de base.

- Permite validar la integración de los distintos componentes y el sistema en conjunto.

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

12.5.4. Auditoría de la fase de construcción

En esta fase se programarán y probarán los distintos componentes y se pondría en marcha todos los procedimientos necesarios para que los usuarios puedan trabajar con el nuevo sistema. Estará basado en las especificaciones físicas obtenidas en la fase de diseño. Hay dos módulos.

12.5.4.1. Desarrollo de los Componentes del Sistema (DCS)

En este módulo se realizarán los distintos componentes, se probarán tanto individualmente como de forma integrada, y se desarrollarán los procedimientos de operación. Se considera un único objetivo de control (serie F):

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

C-F1-1: Se debe preparar adecuadamente el entorno de desarrollo y de pruebas, así como los procedimientos de operación, antes de iniciar el desarrollo. Se debe comprobar que:

- Se han creado e inicializado las bases de datos o archivos necesarios y que cumplen las especificaciones realizadas en el módulo de diseño.
- En ningún momento se trabaja con información que se encuentra en explotación.
- Se han preparado los procedimientos de copia de seguridad.
- Se han preparado los editores, compiladores, herramientas, etc. necesarios.
- Están disponibles los puestos de trabajo y el acceso a los equipos, redes, etc.
- Están disponibles todos los elementos lógicos y físicos para realizar las pruebas unitarias de los componentes y las pruebas de integración.
- Están documentados todos los procedimientos de operación para cuando el sistema esté en explotación.

C-FI-2: Se debe programar, probar y documentar cada uno de los componentes identificados en el diseño del sistema. Se debe comprobar que:

- Se han desarrollado todos los componentes o módulos.
- Se han seguido los estándares de programación y documentación del área, el código es estructurado, está bien sangrado y contiene comentarios suficientes.
- Se ha probado cada componente y se ha generado el informe de prueba. Si los resultados de las pruebas no son satisfactorios, se modifica el código y se vuelve a realizar la prueba. Si se detecta un fallo de especificación o diseño, el proyecto se actualizará según el procedimiento establecido para ello.

C-FI-3: Deben realizarse las pruebas de integración para asegurar que las interfaces, entre los componentes o módulos funcionan correctamente. Se debe comprobar que:

- Las pruebas de integración se han llevado a cabo según lo especificado en el plan de pruebas realizado en el módulo de diseño.
- Se han evaluado las pruebas y se han tomado las acciones correctoras necesarias para solventar las incidencias encontradas, actualizándose el proyecto en consecuencia.
- No han participado los usuarios. En las pruebas de integración sólo debe participar el equipo de desarrollo.

12.5.4.2. Desarrollo de los Procedimientos de Usuario (DPU)

En este módulo se definen los procedimientos y formación necesarios para que los usuarios puedan utilizar el nuevo sistema adecuadamente. Fundamentalmente se trata de la instalación, la conversión de datos y la operación/explotación. Se considera un único objetivo de control (serie G):

OBJETIVO DE CONTROL G1: Al término del proyecto, los futuros usuarios deben estar capacitados y disponer de todos los medios para hacer uso del sistema.

C-G1-1: El desarrollo de los componentes de usuario debe estar planificado. Se debe comprobar que:

- En el plan del proyecto está incluido el plan para el desarrollo de los procedimientos de usuario e incluye todas las actividades y recursos necesarios.

- Los procedimientos se llevan a cabo después de tener la especificación funcional del sistema y antes de la implantación del mismo.

C-G1-2: Se deben especificar los perfiles de usuario requeridos para el nuevo sistema. Se debe comprobar que:

- Están definidos los distintos perfiles de usuario requeridos para la implantación y explotación del nuevo sistema.
- Para cada perfil se ha definido el rango de fechas y la dedicación necesaria.

C-G1-3: Se deben desarrollar todos los procedimientos de usuario con arreglo a los estándares del área. Se debe comprobar que:

- Están desarrollados todos los procedimientos de usuario, recopilados formando el manual de usuario, y son coherentes con las actividades descritas en EFS.
- Cada procedimiento describe claramente qué realiza, el perfil de usuario asociado, así como los recursos que son necesarios (equipos, consumibles, periféricos especiales, espacio, etc.).
- Los manuales de usuario y el resto de procedimientos cumplen los estándares del área y llevan asociado su control de versiones.

C-G1-4: A partir de los perfiles actuales de los usuarios, se deben definir los procesos de formación o selección de personal necesarios. Se debe comprobar que:

- La comparación de perfiles de usuarios y recursos requeridos con los actuales es realista y los procedimientos que se derivan son adecuados y están aprobados por los responsables de las unidades afectadas.
- Los procedimientos de formación están individualizados y se adaptan a cada persona, y se le ha comunicado a cada usuario el plan de formación que seguirá.
- Se han definido y preparado los recursos necesarios para impartir la formación (aulas, medios audiovisuales, material para los asistentes, tutoriales, etc.).

C-G1-5: Se deben definir los recursos materiales necesarios para el trabajo de los usuarios con el nuevo sistema. Se debe comprobar que:

- Se han determinado los recursos necesarios para cada usuario (consumibles, periféricos especiales, espacio, etc.).

- Se han comparado con los recursos existentes y se ha planificado el alquiler, leasing, adquisición, etc. de los recursos no disponibles dentro de plazo.

12.5.5. Auditoría de la fase de implantación

En esta fase se realizará la aceptación del sistema por parte de los usuarios, además de las actividades necesarias para la puesta en marcha. Hay un único módulo:

12.5.5.1. Pruebas, Implantación y Aceptación del Sistema (PIA)

Se verificará en este módulo que el sistema cumple con los requisitos establecidos en la fase de análisis. Una vez probado y aceptado se pondrá en explotación. Se consideran dos objetivos de control (serie H):

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

C-H1-1: Se deben realizar las pruebas del sistema que se especificaron en el diseño del mismo. Se debe comprobar que:

- Se prepara el entorno y los recursos necesarios para realizar las pruebas.

- Las pruebas se realizan y permiten verificar si el sistema cumple las especificaciones funcionales y si interactúa correctamente con el entorno, incluyendo interfaces con otros programas, recuperación ante fallos, copias de seguridad, tiempos de respuesta, etc.

- Se han evaluado los resultados de las pruebas y se han tomado las acciones correctoras necesarias para solventar las incidencias encontradas, actualizándose el proyecto en consecuencia.

IC-H1-2: El plan de implantación y aceptación se debe revisar para adaptarlo a la situación final del proyecto. Se debe comprobar que:

- Se revisa el plan de implantación original y se documenta adecuadamente.

- Está incluida la instalación de todos los componentes desarrollados, así como los elementos adicionales (librerías, utilidades, etc.).

- Incluye la inicialización de datos y la conversión si es necesaria.

- Especifica los recursos necesarios para cada actividad, así como que el orden marcado para las actividades es compatible.

- Se ha tenido en cuenta la información histórica sobre estimaciones.

C-H1-3: El sistema debe ser aceptado por los usuarios antes de ponerse en explotación. Se debe comprobar que:

- Se sigue el plan de pruebas de aceptación aprobado en la fase de análisis, que debe incluir la conversión de datos y la explotación.

- Las pruebas de aceptación son realizadas por los usuarios.

- Se evalúan los resultados de las pruebas y se han tomado las acciones correctoras necesarias para solventar las incidencias encontradas, actualizándose el proyecto en consecuencia.

- El grupo de usuarios y el comité de dirección firman su conformidad con las pruebas de aceptación.

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 todo el entorno en el que se ejecutará.

C-H2-1: Se deben instalar todos los procedimientos de explotación. Se debe comprobar que:

- Se han instalado además del sistema principal todos los procedimientos auxiliares, por ejemplo copias, recuperación, etc., tanto manuales como automáticos.

- Están documentados de forma correcta.

- Los usuarios han recibido la formación necesaria y tienen en su poder toda la documentación necesaria, fundamentalmente manuales de usuario.

- Se han eliminado procedimientos antiguos que sean incompatibles con el nuevo sistema.

C-H2-2: Si existe un sistema antiguo, el sistema nuevo se pondrá en explotación de forma coordinada con la retirada del antiguo, migrando los datos si es necesario. Se debe comprobar que:

- Hay un período de funcionamiento en paralelo de los dos sistemas, hasta que el nuevo sistema esté funcionando con todas las garantías. Esta situación no debe prolongarse más tiempo del necesario.

- Si el sistema antiguo se va a mantener para obtener información se debe dejar en explotación en modo de sólo consulta.

- Los datos se convierten de acuerdo al procedimiento desarrollado y se verifica la consistencia de la información entre el sistema nuevo y el antiguo.

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

- Existe el documento y que ha sido firmado por el comité de dirección y por el grupo de usuarios.

- Contiene de forma explícita la aceptación de la implantación correcta del sistema.

C-H2-4: Se debe supervisar el trabajo de los usuarios con el nuevo sistema en las primeras semanas para evitar situaciones de abandono de uso del sistema. Se debe comprobar que:

- El índice de utilización del sistema es adecuado a los volúmenes que se esperaban para cada una de las áreas afectadas por el nuevo sistema.

- Se ha comprobado, al menos informalmente, la impresión de los usuarios respecto al nuevo sistema.

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

- El mecanismo existe y está aprobado por el director del proyecto, por el comité de dirección y por el área de mantenimiento, si ésta existiese.

- Tiene en cuenta los tiempos de respuesta máximos que se pueden permitir ante situaciones de no funcionamiento.

- El procedimiento a seguir ante cualquier problema o para el mantenimiento del sistema será conocido por todos los usuarios. Incluirá al menos la persona de contacto, teléfono, esquema de la información a aportar, etc.

12.6. CONCLUSIONES

A pesar de ser una de las actividades principales de la informática, el desarrollo de software no ha conseguido alcanzar de forma general unos parámetros de calidad aceptables. Este hecho, unido a la naturaleza especial del software y su difícil validación, convierten al proceso de desarrollo y su estandarización en las claves para cambiar la situación.

Todas las actividades que configuran el proceso de desarrollo tienen la misma importancia a la hora de realizar la auditoría, pues aunque se pueda pensar que la actividad más importante es la programación, se ha demostrado que los errores en las actividades iniciales de los proyectos son más costosos que los que se producen al final de los mismos.

Por otra parte, no parece lógico que los procesos involucrados en el desarrollo de software se estandaricen a lo largo de un proyecto concreto. Es imprescindible que los proyectos de desarrollo se lleven a cabo en el seno de una organización consolidada. Por ello, la organización se convierte en otro elemento crítico a tener en cuenta por el auditor.

Especial mención merecen las nuevas herramientas y técnicas (CASE, programación orientada a objetos, lenguajes de cuarta generación, RAD, prototipado, etc.), que al alterar en cierta medida el proceso tradicional de desarrollo de la ingeniería del software, pasan a ser elementos esenciales a estudiar en un proceso de auditoría.

En este capítulo se han expuesto distintos objetivos de control que de ninguna manera deben interpretarse como un modelo cerrado. El auditor aplicará los objetivos y niveles de cumplimiento mínimos que considere adecuados en función del proyecto y de las peculiaridades de cada organización.

12.7. LECTURAS RECOMENDADAS

Computer Audit, Control and Security. Moeller, R. John Wiley & Sons, 1989.

Técnicas de la auditoría informática. Yann Derrien. Ed. Marcombo, 1994.

Control interno, auditoría y seguridad informática. Coopers & Lybrand, 1996.

Auditoría en centros de cómputo. David H. Li. Ed. Trillas, 1990.

12.8. CUESTIONES DE REPASO

1. ¿Qué factores contribuyen a la importancia de la auditoría de desarrollo?

2. ¿Qué aspectos se deben comprobar respecto a las funciones del área de desarrollo?

3. Comente la importancia, desde el punto de vista de la auditoría, de la formación que deben poseer los profesionales de desarrollo.

4. ¿Qué procedimiento utilizaría para valorar la motivación del personal de desarrollo?

5. ¿Qué repercusiones tiene la existencia de herramientas CASE en el ámbito del desarrollo?

6. Describa diversos procedimientos de Análisis, Evaluación y Selección de herramientas de desarrollo que haya utilizado o conozca.

7. ¿Qué riesgos entraña la subcontratación del desarrollo?

8. ¿Cómo afecta el modelo de ciclo de vida que se adopte en un proyecto a la auditoría a realizar sobre el mismo?

9. ¿Cree que la "trazabilidad" de los requisitos resulta importante en un desarrollo informático?

10. Exponga cómo debería ser la participación del usuario a lo largo de las distintas fases de la metodología Métrica.