Seguridad y Auditoría Informática

Auditoría Informática

Ing. Alfredo Pardo

Año 2021

Tabla de Contenidos

Auditorías de la Dirección de Informática y del Desarrollo

Auditoría de la Dirección de Informática

Las enormes sumas que las empresas dedican a las tecnologías de la información hacen muy necesaria una evaluación independiente de la función que las gestiona.

Se podría decir que algunas de las actividades básicas de todo proceso de dirección son:

- Planificar
- Organizar
- Dirigir
- Controlar

Planificar

Se trata de prever la utilización de las tecnologías de la información en la empresa. Existen varios tipos de planes informáticos. El principal, y origen de todos los demás, lo constituye el Plan Estratégico de Sistemas de Información.

Plan Estratégico de Sistemas de Información

Es el marco básico de actuación de los Sistemas de Información en la empresa. Debe asegurar el alineamiento de los mismos con los objetivos de la propia empresa.
Estos planes no son responsabilidad exclusiva de la Dirección de Informática. Su aprobación final probablemente incumbe a otros estamentos de la empresa: Comité de Informática e incluso en último término de la Dirección General. Sin embargo, la Dirección de Informática debe ser el permanente impulsor de una planificación de Sistemas de Información adecuada y a tiempo.

El entorno en el que se mueve la empresa define el plazo del plan estratégico. Por lo general, este es de 3 a 5 años. Hay muchos factores que influyen: la cultura de la propia empresa, el sector de actividad, las acciones de la competencia, etc.

Guía de Auditoría

El auditor deberá examinar el proceso de planificación de sistemas de información y evaluar si razonablemente se cumplen los objetivos para el mismo. Se deberá evaluar si:

- Durante el proceso de planificación se presta adecuada atención al plan estratégico de la empresa, se establecen mecanismos de sincronización entre sus grandes hitos y los proyectos informáticos asociados y se tienen en cuenta aspectos como cambios organizativos, entorno legislativo, evolución tecnológica, organización informática, recursos, etc., y sus impactos están adecuadamente reflejados en el Plan Estratégico de Sistemas de Información.
- Las tareas y actividades presentes en el Plan tienen la correspondiente y adecuada asignación de recursos para poder llevarlas a cabo. Asimismo, si tienen plazos de consecución realistas en función de la situación actual de la empresa, de la organización informática, del estado de la tecnología, etc.

Entre las acciones a realizar, se pueden describir:

- Lectura de actas de sesiones del Comité de Informática dedicadas a la planificación estratégica.
- Identificación y lectura de los documentos intermedios prescritos por la metodología de planificación.
- Lectura y comprensión detallada del Plan e identificación de las consideraciones incluidas en el mismos sobre los objetivos empresariales, cambios organizativos, evolución tecnológica, plazos y niveles de recursos, etc.
- Realización de entrevistas al Director de Informática y a otros miembros del Comité de Informática participantes en el proceso de elaboración del Plan Estratégico. Igualmente, realización de entrevistas a representantes de los usuarios con el fin de evaluar su grado de participación y sintonía con el contenido del Plan.
- Identificación y comprensión de los mecanismos existentes de seguimiento y actualización del Plan y de su relación con la evolución de la empresa.

Otros planes relacionados

Normalmente, deben existir otros planes informáticos, todos ellos nacidos al amparo del Plan Estratégico. Entre otros, los más habituales suelen ser:

- Plan operativo anual
- Plan de dirección tecnológica
- Plan de arquitectura de la información

- Plan de recuperación ante desastres

Algunos de ellos (Plan tecnológico, Plan de arquitectura) aparecen a veces integrados en el propio Plan Estratégico.

Plan Operativo Anual

El Plan operativo de Sistemas de Información describe las actividades a realizar durante el siguiente ejercicio natural. Entre otros aspectos, debe señalar los sistemas de información a desarrollar, los cambios tecnológicos previstos, los recursos y los plazos necesarios, etc.

El auditor deberá evaluar la existencia del Plan y su nivel de calidad. Deberá estudiar su alineamiento con el Plan Estratégico, su grado de atención a las necesidades de los usuarios, sus previsiones de los recursos necesarios para llevar a cabo el Plan, etc. Deberá analizar si los plazos descritos son realistas teniendo en cuenta, entre otras cosas, las experiencias anteriores en la empresa, etc.

Plan de Recuperación ante Desastres

Una instalación informática puede verse afectada por desastres de variada naturaleza: incendio, inundación, fallo de algún componente crítico de hardware, robo, sabotaje, acto de terrorismo, etc. que tengan como consecuencia inmediata la indisponibilidad de un servicio informático adecuado. La Dirección debe prever esta posibilidad y, por tanto, planificar para hacer frente.

Organizar y Dirigir

El proceso de organizar sirve para estructurar los recursos, los flujos de información y los controles que permitan alcanzar los objetivos marcados durante la planificación.

Comité de Informática

El Comité de Informática es el primer lugar de encuentro dentro de la empresa de los informáticos y sus usuarios: es el lugar en el que se debaten los grandes asuntos de la informática que afectan a toda la empresa y permite a los usuarios conocer las necesidades del conjunto de la organización y participar en la fijación de prioridades.

La Dirección de Informática debe ser el principal impulsor de la existencia del Comité. Éste debería estar formado por pocas personas y presidido por el director con mayor experiencia dentro de la empresa, responsable en último término por las tecnologías de la información.

El Director de Informática debería actuar como secretario del Comité y las grandes áreas usuarias deberían estar representadas al nivel de sus directores con mayor experiencia.

Asimismo, el director de Auditoría Interna debería ser miembro del Comité. Otras personas de la organización también pueden integrarse en el Comité como miembros temporales cuando se traten asuntos de su incumbencia o de su especialidad.

Las funciones del Comité de Informática deberían ser:

- Aprobación del Plan Estratégico de Sistemas de Información.
- Aprobación de las grandes inversiones en tecnología de la información.
- Fijación de prioridades entre los grandes proyectos informáticos.
- Vehículo de discusión entre la Informática y sus usuarios.
- Vigila y realiza el seguimiento de la actividad del Departamento de Informática.

Al tratarse del máximo órgano decisorio sobre el papel de las tecnologías de información en la empresa, ninguna auditoría de la Dirección de Informática debería soslayar su revisión. El auditor deberá asegurar que el Comité de Informática existe y cumple su papel adecuadamente.

Entre las acciones a realizar figuran:

- Lectura de la normativa interna, si la hubiera, para conocer las funciones que debería cumplir el Comité de Informática.
- Entrevistas a miembros destacados del Comité con el fin de conocer las funciones que en la práctica realiza dicho Comité.
- Entrevistas a los representantes de los usuarios, miembros del Comité, para conocer si entienden y están de acuerdo con su papel en el mismo.

Una vez establecida la existencia del Comité de Informática, habrá que evaluar la adecuación de las funciones que realiza. Para ello, el auditor, mediante un conjunto de entrevistas, lecturas de documentación interna del Comité, etc., deberá establecer un juicio sobre la validez, adecuación, etc. de las actuaciones del Comité.

Entre las acciones a realizar figuran:

- Lectura de las actas del Comité y entrevistas a los miembros del mismo, con especial incidencia en los representantes de los usuarios para comprobar que:
    - El Comité cumple efectivamente con las funciones enunciadas.
    - Los acuerdos son tomados correctamente y los puntos de vista de los representantes de los usuarios son tenidos en cuenta.

Posición del Departamento de Informática en la Empresa

El Departamento de Informática debería estar suficientemente alto en la jerarquía y contar con masa crítica suficiente para disponer de autoridad e independencia frente a los departamentos usuarios.

Es cada vez más habitual encontrar a departamentos de informática dependiendo directamente de la Dirección General. Incluso, en las grandes organizaciones, el Director de Informática es por defecto miembro del Comité de Dirección u órgano semejante. Siempre que el departamento de informática esté integrado en algún departamento usuario, pueden surgir dudas razonables sobre su equidad a la hora de atender las peticiones del resto de departamentos de la empresa.

El auditor debe evaluar si las necesidades de los diferentes departamentos de la empresa son tratadas equitativamente por Informática y no existe un sesgo demasiado alto hacia un departamento de la misma. Si esto ocurriera, una de las primeras razones para ello puede ser la ubicación incorrecta de dicho Departamento.

Guía de auditoría

El auditor deberá revisar el emplazamiento organizativo del Departamento de Informática y evaluar su independencia frente a departamentos usuarios. Para este proceso, será muy útil realizar entrevistas con el Director de Informática y directores de algunos departamentos usuarios para conocer su percepción sobre el grado de independencia y atención del Departamento de Informática.

Descripción de Funciones y Responsabilidades del Departamento de Informática

Segregación de Funciones

Es necesario que las grandes unidades organizativas dentro del Departamento de Informática tengan sus funciones descritas y sus responsabilidades claramente delimitadas y

documentadas. Igualmente, es necesario que este conocimiento se extienda a todo el personal perteneciente a Informática: todos ellos deben conocer sus funciones y responsabilidades en relación con los sistemas de información. Todo ello es una labor de la Dirección de Informática.

La filosofía básica que debe orientar la separación de funciones es impedir que un solo individuo pueda trastornar un proceso crítico. Además, se debería asegurar que el personal de Informática actúa únicamente dentro de la descripción de las funciones existente para su puesto de trabajo concreto.

Se debería asegurar la segregación entre las funciones de desarrollo de sistemas de información, la de producción o funcionamiento y los departamentos de usuarios. Además, la función de administración de la seguridad debería estar claramente separada de la de producción.

Aseguramiento de la Calidad

La calidad de los servicios ofrecidos por el Departamento de Informática debe estar asegurada mediante el establecimiento de una función organizativa de Aseguramiento de la Calidad. Esta función de control debe ser independiente de la actividad diaria del departamento y debe depender directamente de la Dirección de Informática.

Guía de auditoría

El auditor deberá comprobar que las descripciones están documentadas y son actuales y que las unidades organizativas informáticas las comprenden y desarrollan su labor de acuerdo a las mismas.

Entre las tareas que el auditor podrá realizar, figuran:

- Examen del organigrama del Departamento de Informática e identificación de las grandes unidades organizativas.
- Revisión de la documentación existente para conocer la descripción de las funciones y responsabilidades.
- Realización de entrevistas a los directores de cada una de las grandes unidades organizativas para determinar su conocimiento de las responsabilidades de su unidad y que éstas responden a las descripciones existentes en la documentación correspondiente.
- Examen de las descripciones de las funciones para evaluar si existe adecuada segregación de funciones, incluyendo la separación entre desarrollo de sistemas de

información, producción y departamentos usuarios. Igualmente, será menester evaluar la independencia de la función de seguridad.
- Observación de las actividades del personal del Departamento para analizar, en la práctica, las funciones realizadas, la segregación entre las mismas y el grado de cumplimiento con la documentación analizada.

Aseguramiento de la Calidad

El auditor deberá evaluar la independencia de la función frente al resto de las áreas operativas del Departamento de Informática, su dotación de recursos humanos, la experiencia de los mismos, la existencia de métodos y procedimientos formales de actuación, las posibilidades reales de realizar su trabajo, el contenido de los informes elaborados por la función, etc.

Entre las acciones a llevar a cabo, se pueden considerar:
- Conocimiento de la posición de la Función en el organigrama del Departamento de Informática.
- Análisis del grado de cumplimiento de las actividades del Departamento en relación con las políticas, estándares y procedimientos existentes tanto generales del Departamento como específicos de sus funciones organizativas.
- Revisión de algunos informes emitidos por la Función con el fin de evaluar si su estructura y contenido son adecuados. Analizar la existencia de acciones de seguimiento basadas en dichos informes.

Estándares de Funcionamiento y Procedimientos. Descripción de los Puestos de Trabajo

Deben existir estándares de funcionamiento y procedimientos que gobiernen la actividad del Departamento de Informática, por un lado, y sus relaciones con los departamentos usuarios por otro. Estos estándares son el vehículo ideal para transmitir al personal de Informática la filosofía, mentalidad y actitud hacia los controles necesarios con la finalidad de crear y mantener un entorno controlado para la vida de los sistemas de información de la empresa.

Estos estándares y procedimientos deben estar documentados, actualizados y ser comunicados adecuadamente a todos los departamentos afectados. La Dirección de Informática debe promover la adopción de estándares y procedimientos y dar ejemplo de su uso.

Por otro lado, deben existir documentadas descripciones de los puestos de trabajo dentro de Informática delimitando claramente la autoridad y responsabilidad en cada caso. Las

descripciones deberían incluir los conocimientos técnicos y/o experiencia necesarios para cada puesto de trabajo.

Guía de auditoría

El auditor deberá evaluar la existencia de estándares de funcionamiento y procedimientos y descripciones de puestos de trabajo adecuados y actualizados.

Entre las acciones a realizar, se pueden citar:

- Evaluación del proceso por el que los estándares, procedimientos y puestos de trabajo son desarrollados, aprobados, distribuidos y actualizados.
- Revisión de los estándares y procedimientos existentes para evaluar si transmiten y promueven una filosofía adecuada de control. Evaluación de su adecuación, grado de actualización, y nivel de cobertura de las actividades informáticas y de las relaciones con los departamentos usuarios.
- Revisión de las descripciones de los puestos de trabajo para evaluar si reflejan las actividades realizadas en la práctica.

Gestión Económica

Presupuestación

El Departamento de Informática debe tener un presupuesto económico, normalmente en base anual, el cual debe desarrollarse basado en la política seguida en la empresa sobre si los costos de tecnología forman parte del departamento o si éstos deben ser pagados por los departamentos usuarios.

El auditor deberá juzgar si los métodos de presupuestación son apropiados. En todo proceso de presupuestación de un Departamento de Informática debe haber una previa petición de necesidades a los departamentos usuarios. Adicionalmente, el Departamento tendrá sus propias necesidades que se deberán integrar en el presupuesto. Lo más lógico es elaborar al mismo tiempo el presupuesto económico y el Plan operativo anual.

Guía de Auditoría

El auditor deberá constatar la existencia de un presupuesto económico, de un proceso para elaborarlo -que incluya consideraciones de los usuarios- y aprobarlo, y que dicho proceso está en línea con las políticas y procedimientos de la empresa y con los planes estratégico y operativo del propio Departamento.

Adquisición de bienes y servicios

Los procedimientos que el Departamento de Informática siga para adquirir los bienes y servicios descritos en su plan operativo anual y/o que se demuestren necesarios a lo largo del ejercicio deben estar documentados y alineados con los procedimientos de compras del resto de la empresa.

Guía de Auditoría

El auditor deberá seguir las directrices y programas de trabajo de auditoría elaborados para el proceso de compras establecido por la empresa.

Medida y reparto de costos

La Dirección de Informática debe en todo momento gestionar los costos asociados con la utilización de los recursos informáticos: humanos y tecnológicos. Esto exige medirlos. La existencia o ausencia de un sistema de este tipo suele estar asociada a la propia cultura de la empresa.

Guía de Auditoría

El precio de transferencia es el costo interno que el Departamento de Informática repercute a los departamentos usuarios por los servicios que les presta.

El auditor deberá evaluar la conveniencia de que exista o no un sistema de reparto de costos informáticos y de que éste sea justo, incluya los conceptos adecuados y de que el precio de transferencia aplicado esté en línea o por debajo del disponible en el mercado.

Entre las acciones a llevar a cabo, se pueden mencionar:

- Realización de entrevistas a la dirección de los departamentos usuarios para evaluar su grado de comprensión de los componentes de costo utilizados en la fórmula de cálculo del precio de transferencia.
- Análisis de los componentes y criterios con los que está calculado el precio de transferencia para evaluar su ecuanimidad y consistencia, y acudir al mercado externo y a ofertas de centros de proceso de datos independientes para compararlas con dichos costos internos.
- Conocimiento de los diversos sistemas existentes en el Departamento para recoger y registrar la actividad del mismo (consumo de recursos de máquina, número de líneas

impresas, horas de programación, de help-desk, etc.), para procesarla y obtener la información de costos y para presentarla de una manera apropiada.

Controlar

Control y Seguimiento

La Dirección tiene la obligación de controlar y efectuar un seguimiento permanente de las distintas actividades del Departamento. Se debe vigilar el desarrollo de los planes estratégico y operativo y de los proyectos que los desarrollan, la ejecución del presupuesto, la evolución de la cartera de peticiones de usuario pendientes, la evolución de los costos, los planes de formación, la evolución de la carga del computador y de los otros recursos (espacio en disco, comunicaciones, capacidad de las impresoras, etc.).

En esta tarea, es conveniente que existan estándares de rendimiento con los que comparar las diversas tareas. Son aplicables a las diversas facetas de la actividad del Departamento: consumo de recursos del equipo, desarrollo, operaciones, etc.

Guía de auditoría

Entre las acciones a realizar, se pueden mencionar:

- Conocimiento y análisis de los procesos existentes en el Departamento para llevar a cabo el seguimiento y control. Evaluación de la periodicidad de los mismos. Analizar igualmente los procesos de presupuestación.
- Revisión de planes, proyectos, presupuestos de años anteriores y del actual para comprobar que son estudiados, que se analizan las desviaciones y que se toman las medidas correctoras necesarias.

Cumplimiento de la normativa legal

La Dirección de Informática debe controlar que la realización de sus actividades se lleva a cabo dentro del respeto a la normativa legal aplicable. En particular, se consideran fundamentales los relativos a la seguridad e higiene en el trabajo, normativa laboral y sindical, protección de datos personales, propiedad intelectual del software, requisitos definidos en la cobertura de seguros, contratos de comercio electrónico, transmisión de datos por líneas de comunicaciones, así como normativa emitida por órganos reguladores sectoriales.

Asimismo, deben existir procedimientos para vigilar y determinar permanentemente la legislación aplicable.

Guía de auditoría

El auditor deberá evaluar si la mencionada normativa aplicable se cumple.

Para ello, deberá, en primer lugar, entrevistarse con la Asesoría Jurídica de la empresa, la Dirección de Recursos Humanos y la Dirección de Informática con el fin de conocer dicha normativa.

A continuación, evaluará el cumplimiento de las normas. Si el auditor no es un técnico en los distintos aspectos legales, deberá buscar asesoramiento adecuado interno a la empresa o externo.

Auditoría del Desarrollo

Introducción

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. El desarrollo incluye todo el ciclo de vida del software excepto la funcionamiento, el mantenimiento y la retirada de servicio de las aplicaciones cuando ésta tenga lugar.

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 los principios de ingeniería de software o, por el contrario, determinar las deficiencias existentes en este sentido.

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

- Planificación del área y participación 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 implementación. El mantenimiento se supondrá una 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 asignado al área.
- Establecimiento de normas y controles para todas las actividades que se realizan en el área y comprobación de su cumplimiento.

Una vez conocidas las tareas que se realizan en el área de desarrollo, se abordará la auditoría de la misma en dos grandes apartados:

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

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 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.

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 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.

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. Se consideran ocho objetivos de control:

Objetivo de Control 1: El área de desarrollo debe tener funciones asignadas dentro del departamento y una organización que le permita el cumplimiento de los mismos.

Controles:

1. Deben establecerse de forma clara las funciones del área de desarrollo dentro del departamento de informática.
2. Debe especificarse el organigrama con la relación de puestos del área, así como el personal asignado y puesto que ocupa cada persona. Debe existir un procedimiento para la promoción del personal.
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.
4. El área de desarrollo llevará su propio control presupuestario.

Objetivo de Control 2: El personal del área de desarrollo debe contar con la formación adecuada y estar motivado para la realización de su trabajo.

Controles:

1. Deben existir procedimientos de contratación objetivos.
2. Debe existir un plan de formación que esté en consonancia con los objetivos tecnológicos que se tengan en el área.
3. Debe existir un protocolo de recepción/abandono para las personas que se incorporan o dejan el área.
4. Deben existir medios físicos o digitales de capacitación accesibles por el personal del área.
5. El personal debe estar motivado en la realización de su trabajo. Este aspecto es difícil de valorar y no es puramente técnico.

Objetivo de Control 3: Si existe un plan de sistemas, los proyectos que se lleven a cabo se basarán en dicho plan y lo mantendrán actualizado.

Controles:

1. La realización de nuevos proyectos debe basarse en el plan de sistemas en cuanto a objetivos, marco general y horizonte temporal.
2. El plan de sistemas debe actualizarse con la información que se genera a lo largo de un proceso de desarrollo.

Objetivo de Control 4: La propuesta y aprobación de nuevos proyectos debe realizarse siguiendo reglas preestablecidas.

Controles:

1. Debe existir un procedimiento para la propuesta de realización de nuevos proyectos.
2. Debe existir un procedimiento de aprobación de nuevos proyectos que dependerá de que exista o no plan de sistemas.

Objetivo de Control 5: La asignación de recursos a los proyectos debe basarse en reglas preestablecidas.

Controles:

1. Debe existir un procedimiento para asignar director y equipo de desarrollo a cada nuevo proyecto.
2. Debe existir un procedimiento para conseguir los recursos materiales necesarios para cada proyecto.

Objetivo de Control 6: El desarrollo de sistemas de información debe hacerse aplicando principios de ingeniería del software ampliamente aceptados.

Controles:

1. Debe tenerse implantada una metodología de desarrollo de sistemas de información soportada por herramientas de ayuda (CASE).
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 clásicos.
3. Los lenguajes, compiladores, herramientas CASE, software de control de versiones, etc. usados en el área deben ser previamente homologados.
4. Debe practicarse la reutilización del software.
5. Debe existir un método que permita catalogar y estimar los tiempos de cada una de las fases de los proyectos.
6. Debe existir un registro de problemas que se producen en los proyectos del área, incluyendo los fracasos de proyectos completos.

Objetivo de Control 7: Las relaciones con el exterior del departamento tienen que producirse de acuerdo a un procedimiento.

Controles:

1. Deben mantenerse contactos con proveedores para recibir información suficiente sobre productos que puedan ser de interés.
2. Debe existir un protocolo para la contratación de servicios externos.

Objetivo de Control 8: La organización del área debe estar siempre adaptada a las necesidades de cada momento.

Controles:

1. La organización debe revisarse de forma regular.

Auditoría de Proyectos de Desarrollo de S.I. (Fases)

Cada desarrollo de un nuevo sistema de información será un proyecto con entidad propia. El proyecto tendrá 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.
Dentro del desarrollo de sistemas de información se han propuesto cinco subdivisiones, entre las cuales se encuentran: análisis, diseño, construcción e implementación.
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.

Aprobación, Planificación y Gestión del Proyecto

Se consideran en este apartado dos objetivos de control:

Objetivo de Control 1: El proyecto de desarrollo deberá estar aprobado, definido y planificado formalmente.

Controles:

1. Debe existir una orden de aprobación del proyecto que defina claramente los objetivos, restricciones y las unidades afectadas.
2. Debe designarse a un responsable o director del proyecto.
3. El proyecto debe ser catalogado y, en función de sus características, se debe determinar el modelo de ciclo de vida que seguirá.
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.

Objetivo de Control 2: 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.

Controles:

1. Los responsables de las unidades o áreas afectadas por el proyecto deben participar en la gestión del proyecto.

2. Se debe establecer un mecanismo para la resolución de los problemas que puedan plantearse a lo largo del proyecto.
3. Debe existir un control de cambios a lo largo del proyecto.
4. Cuando sea necesario reajustar el plan del proyecto, normalmente al finalizar un módulo o fase, debe hacerse de forma adecuada.
5. Debe hacerse un seguimiento de los tiempos empleados tanto por tarea como a lo largo del proyecto.
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.
7. Cuando termina el proyecto se debe cerrar toda la documentación del mismo, liberar los recursos empleados y hacer balance.

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 forma independiente del entorno técnico. Esta fase se divide en dos módulos.

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 estos requisitos y de entre ellas se elegirá la más adecuada. Se consideran dos objetivos de control.

Objetivo de Control 1: Los usuarios y responsables de las unidades a las que afecta el nuevo sistema establecerán de forma clara los requisitos del mismo.

Controles:

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.
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.

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

Objetivo de Control 2: En el proyecto de desarrollo se utilizará la alternativa más favorable para conseguir que el sistema cumpla los requisitos establecidos.

Controles:

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.
2. La actualización del plan de proyecto seguirá los criterios preestablecidos.

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 los 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.

Objetivo de Control 1: El nuevo sistema debe especificarse de forma completa desde el punto de vista funcional, contando esta especificación con la aprobación de los usuarios.

Controles:

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.
2. Debe existir el diccionario de datos o repositorio.
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.

4. La especificación del nuevo sistema incluirá los requisitos de seguridad, rendimiento, copias de seguridad y recuperación, etc.
5. Se deben especificar las pruebas que el nuevo sistema debe superar para ser aceptado.
6. La actualización del plan de proyecto seguirá los criterios ya establecidos, detallando en este punto en mayor medida la entrega y transición al nuevo sistema.

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.

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.

Objetivo de Control 1: Se debe definir una arquitectura física para el sistema coherente con la especificación funcional que se tenga y con el entorno tecnológico elegido.

Controles:
1. El entorno tecnológico debe estar definido de forma clara y ser conforme a los estándares del departamento de informática.
2. Se deben identificar todas las actividades físicas a realizar por el sistema y descomponer las mismas de forma modular.
3. Se debe diseñar la estructura física de datos adaptando las especificaciones del sistema al entorno tecnológico.
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.
5. La actualización del plan de proyecto seguirá los criterios previamente especificados.

Auditoría de la Fase de Construcción

En esta fase se desarrollarán y probarán los distintos componentes y se pondrán 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. Tiene dos módulos.

Desarrollo de 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.

Objetivo de Control 1: Los componentes o módulos deben desarrollarse usando técnicas de programación correctas.

Controles:

1. Se debe preparar adecuadamente el entorno de desarrollo y de pruebas, así como los procedimientos de operación, antes de iniciar el desarrollo.
2. Se debe programar, probar y documentar cada uno de los componentes identificados en el diseño del sistema.
3. Deben realizarse las pruebas de integración para asegurar que las interfaces entre los componentes o módulos funcionan correctamente.

Desarrollo de 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/funcionamiento. Se considera un único objetivo de control.

Objetivo de Control 1: Al término del proyecto, los futuros usuarios deben estar capacitados y disponer de todos los medios para hacer uso del sistema.

Controles:

1. El desarrollo de los componentes de usuario debe estar planificado.
2. Se deben especificar los perfiles de usuario requeridos para el nuevo sistema.
3. Se deben desarrollar todos los procedimientos de usuario de acuerdo a los estándares del área.
4. A partir de los perfiles actuales de los usuarios, se deben definir los procesos de información o selección de personal necesarios.
5. Se deben definir los recursos materiales necesarios para el trabajo de los usuarios con el nuevo sistema.

Auditoría de la Fase de Implementación

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.

Pruebas, Implementación 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 funcionamiento. Se consideran dos objetivos de control.

Objetivo de Control 1: El sistema debe ser aceptado formalmente por los usuarios antes de ser puesto en funcionamiento.

Controles:

1. Se deben realizar las pruebas del sistema que se especificaron en el diseño del mismo.
2. El plan de implementación y aceptación se debe revisar para adaptarlo a la situación final del proyecto.
3. El sistema debe ser aceptado por los usuarios antes de ponerse en funcionamiento.

Objetivo de Control 2: El sistema se pondrá en funcionamiento formalmente y pasará a estar en mantenimiento sólo cuando haya sido aceptado y esté preparado todo el entorno en el que se ejecutará.

Controles:

1. Se deben instalar todos los procedimientos de funcionamiento.
2. Si existe un sistema antiguo, el sistema nuevo se pondrá en funcionamiento de forma coordinada con la retirada del antiguo, migrando los datos si es necesario.
3. Debe firmarse el final de la implementación por parte de los usuarios.
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.
5. Para terminar el proyecto se pondrá en marcha el mecanismo de mantenimiento.